Junos® OS

CLI Reference

Release

11.1

Published: 2011-02-09

Copyright © 2011, Juniper Networks, Inc.

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® OS CLI Reference
Release 11.1
Copyright © 2011, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
February 2011—R1 Junos OS 11.1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

Copyright © 2011, Juniper Networks, Inc.

12. **Commercial Computer Software.** The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html .

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Copyright © 2011, Juniper Networks, Inc.

Table of Contents

About This Guide . . . xxxix

J Series and SRX Series Documentation and Release Notes . . . xxxix
Objectives . . . xl
Audience . . . xl
Supported Routing Platforms . . . xl
Document Conventions . . . xl
Documentation Feedback . . . xlii
Requesting Technical Support . . . xlii
Self-Help Online Tools and Resources . . . xliii
Opening a Case with JTAC . . . xliii

Part 1 Configuration Statements

Chapter 1 **Access Hierarchy and Statements . . . 3**

Access Configuration Statement Hierarchy . . . 3
address-assignment . . . 8
address-pool . . . 10
admin-search . . . 11
assemble . . . 11
authentication-order . . . 12
banner (FTP, HTTP, Telnet) . . . 12
banner (Web Authentication) . . . 13
base-distinguished-name . . . 14
client-group . . . 15
client-idle-timeout . . . 15
client-name-filter . . . 16
client-session-timeout . . . 16
configuration-file . . . 17
count . . . 17
default-profile . . . 18
dhcp-attributes (IPv4) . . . 19
dhcp-attributes (IPv6) . . . 20
distinguished-name . . . 21
domain-name . . . 21
fail . . . 22
firewall-authentication . . . 23
firewall-user . . . 24
ftp . . . 24
group-profile . . . 25
http . . . 26
ip-address . . . 26

Copyright © 2011, Juniper Networks, Inc.

ldap-options . . . 27
ldap-server . . . 28
link . . . 28
login . . . 29
name-server (address-assignment pool) . . . 29
neighbor-discovery-router-advertisement . . . 30
network . . . 30
pass-through . . . 31
password . . . 32
pool (Address-Assignment Pools) . . . 33
port (LDAP) . . . 34
port (RADIUS) . . . 35
prefix . . . 35
profile . . . 36
radius-options . . . 37
radius-server . . . 38
range . . . 39
retry (LDAP) . . . 39
retry (RADIUS) . . . 40
revert-interval (LDAP) . . . 40
revert-interval (RADIUS) . . . 41
routing-instance (LDAP) . . . 41
routing-instance (RADIUS) . . . 42
search . . . 42
search-filter . . . 43
secret . . . 43
securid-server . . . 44
separator . . . 45
session-options . . . 45
source-address (LDAP) . . . 46
source-address (RADIUS) . . . 46
success . . . 47
telnet . . . 47
timeout (LDAP Server) . . . 48
timeout (RADIUS Server) . . . 48
traceoptions . . . 49
xauth-attributes . . . 50
web-authentication . . . 51
wins-server . . . 51

Chapter 2 Accounting-Options Hierarchy . . . 53

Accounting-Options Configuration Statement Hierarchy . . . 53

Chapter 3 Application Hierarchy and Statements . . . 55

Applications Configuration Statement Hierarchy . . . 55
alg . . . 57
application-protocol . . . 58
destination-port . . . 59
icmp-code . . . 63
icmp-type . . . 63

 Copyright © 2011, Juniper Networks, Inc.

inactivity-timeout 64
protocol 65
rpc-program-number 66
source-port 66
term 67
uuid 68

Chapter 4 Bridge-Domains Hierarchy and Statements 69

Bridge-Domains Configuration Statement Hierarchy 69
bridge-domains 70
bridge-options 71
domain-type 71
interface 72
routing-interface 72
static-mac 73
vlan-id 73
vlan-id-list 74

Chapter 5 Chassis Hierarchy and Statements 75

Chassis Configuration Statement Hierarchy 75
cluster 79
control-link-recovery 80
control-ports 81
framing 81
global-threshold 82
global-weight 83
gratuitous-arp-count 84
heartbeat-interval 85
heartbeat-threshold 86
hold-down-interval 87
interface 88
interface-monitor 89
ip-monitoring 90
network-management 91
node (Cluster) 91
node (Redundancy-Group) 92
pic-mode 93
pic-mode (Channel) 94
preempt 94
priority 95
redundancy-group 96
retry-count 97
retry-interval 98
reth-count 98
traceoptions 99
tunnel-queuing 100
weight 101

Chapter 6 **Class-of-Service Hierarchy and Statements 103**

Class-of-Service Configuration Statement Hierarchy 103
adaptive-shaper 106
adaptive-shapers 107
classifiers 108
code-points (Forwarding Class) 109
default 109
frame-relay-de (Assigning to an Interface) 110
frame-relay-de (Defining Loss Priority) 111
frame-relay-de (Defining Rewrite Rule) 112
forwarding-classes 112
interface (class-of-service) 113
loss-priority (Frame Relay DE Bit Loss-Priority Map) 114
loss-priority (Rewrite Rules) 115
loss-priority-maps (Assigning to an Interface) 116
loss-priority-maps (Defining) 116
rewrite-rules (Definition) 117
rewrite-rules (Interfaces) 118
scheduler-map (Virtual Channels) 119
shaping-rate (Adaptive Shaping) 120
shaping-rate (Applying to an Interface) 121
shaping-rate (Virtual Channels) 122
trigger 122
virtual-channels 123
virtual-channel-group 124
virtual-channel-groups 125

Chapter 7 **Event-Options Hierarchy 127**

Event-Options Configuration Statement Hierarchy 127

Chapter 8 **Firewall Hierarchy and Statements 129**

Firewall Configuration Statement Hierarchy 129
policer 132
simple-filter 133

Chapter 9 **Forwarding-Options Hierarchy and Statements 135**

Forwarding-Options Configuration Statement Hierarchy 135
hash-key 139
vpn 140

Chapter 10 **Groups Hierarchy 141**

Groups Configuration Statement Hierarchy 141

Chapter 11 **Interfaces Hierarchy and Statements 143**

Interfaces Configuration Statement Hierarchy 143
access-point-name 156
activation-priority 156
annex 157
authentication-method 157
bandwidth 158
bearer-bandwidth-limit 158

 Copyright © 2011, Juniper Networks, Inc.

bundle . . . 159
cbr rate . . . 159
cellular-options . . . 160
client-identifier . . . 160
compression-device . . . 161
credit . . . 161
dhcp . . . 162
dynamic-call-admission-control . . . 163
encapsulation . . . 164
fabric-options . . . 164
family bridge . . . 165
family inet . . . 166
family inet6 . . . 167
flag . . . 168
flow-control . . . 169
fpc . . . 169
gsm-options . . . 170
interface (PIC Bundle) . . . 170
lacp . . . 171
latency . . . 171
lease-time . . . 172
line-rate . . . 172
link-speed . . . 173
loopback . . . 173
media-type . . . 174
member-interfaces . . . 174
minimum-links . . . 175
native-vlan-id . . . 175
next-hop-tunnel . . . 176
no-flow-control . . . 176
no-loopback . . . 176
no-source-filtering . . . 176
periodic . . . 177
pic-mode . . . 178
profiles . . . 179
promiscuous-mode . . . 179
quality . . . 180
radio-router . . . 180
redundancy-group . . . 181
redundant-ether-options . . . 181
redundant-parent (Fast Ethernet Options) . . . 182
redundant-parent (Gigabit Ethernet Options) . . . 182
resource . . . 183
retransmission-attempt . . . 183
retransmission-interval . . . 184
roaming-mode . . . 184
select-profile . . . 185
server-address . . . 185
simple-filter . . . 186

Copyright © 2011, Juniper Networks, Inc.

sip-password . . . 186
sip-user-id . . . 187
source-address-filter . . . 187
source-filtering . . . 188
speed . . . 188
threshold . . . 189
traceoptions . . . 189
update-server . . . 190
unframed | no-unframed . . . 190
vbr rate . . . 191
vdsl-profile . . . 192
vendor-id . . . 192
vlan-tagging . . . 193
web-authentication . . . 193

Chapter 12 Power Over Ethernet Hierarchy and Statements . . . 195

PoE Configuration Statement Hierarchy . . . 195
disable . . . 196
duration . . . 196
guard-band . . . 197
interface . . . 198
interval . . . 199
management . . . 199
maximum-power . . . 200
priority . . . 201
telemetries . . . 202

Chapter 13 Policy-Options Hierarchy and Statements . . . 203

Policy-Options Configuration Statement Hierarchy . . . 203
condition . . . 204
route-active-on . . . 205

Chapter 14 Protocols Hierarchy and Statements . . . 207

Protocols Configuration Statement Hierarchy . . . 207
disable . . . 229
end-system-configuration-timer . . . 230
esis . . . 230
graceful-restart . . . 231
hold-time . . . 231
interface . . . 232
global-mac-limit . . . 232
global-mac-table-aging-time . . . 233
global-no-mac-learning . . . 233
l2-learning . . . 234
packet-action . . . 234
preference . . . 235
traceoptions . . . 236

Chapter 15 Routing-Instances Hierarchy . . . 239

Routing-Instances Configuration Statement Hierarchy . . . 239

 Copyright © 2011, Juniper Networks, Inc.

Chapter 16 **Routing-Options Hierarchy 249**

Routing-Options Configuration Statement Hierarchy 249

Chapter 17 **Schedulers Hierarchy and Statements 257**

Schedulers Configuration Statement Hierarchy 257
all-day 258
daily 259
exclude 259
friday 260
monday 261
saturday 262
scheduler 263
schedulers 264
start-date 264
start-time 265
stop-date 266
stop-time 267
sunday 268
thursday 269
tuesday 270
wednesday 271

Chapter 18 **Security Hierarchy and Statements 273**

Security Configuration Statement Hierarchy 273
access-profile (Dynamic VPNs) 309
access-profile (IPsec VPNs) 309
ack-number 310
action 311
action (Application-Level DDoS) 312
action (web filtering) 313
active-policy 313
action-profile 314
address (ARP Proxy) 315
address (Destination NAT) 315
address (IKE Gateway) 316
address (Zone Address Book) 317
address-book 318
address-blacklist 318
address-mapping 319
address-persistent 319
address-set 320
address-whitelist 320
admin-email 321
administrator 321
administrator-email (fallback-block) 322
administrator-email (virus-detection) 322
aging 323
alarm-threshold 323
alarm-without-drop 324

Copyright © 2011, Juniper Networks, Inc.

alert . . . 324
alg . . . 325
algorithm . . . 329
all-tcp . . . 329
allow-dns-reply . . . 330
allow-email (fallback-block) . . . 330
allow-email (virus-detect) . . . 331
allow-icmp-without-flow . . . 331
always-send . . . 331
analysis no-reports . . . 332
anomaly . . . 332
antispam (feature-profile) . . . 333
antispam (utm-policy) . . . 334
antivirus (feature-profile) . . . 335
antivirus (utm-policy) . . . 337
apn (gtp) . . . 338
application (Application-Level DDoS) . . . 339
application (Protocol Binding Custom Attack) . . . 339
application (Security Policies) . . . 340
application-firewall . . . 341
application-identification . . . 342
application-screen (H323) . . . 343
application-screen (MGCP) . . . 343
application-screen (SCCP) . . . 344
application-screen (SIP) . . . 345
application-services (Application Firewall) . . . 346
application-services (Priority) . . . 347
application-services (Unified Access Control) . . . 348
application-services (WXC Integrated Services Module) . . . 348
application-system-cache . . . 349
application-system-cache-timeout . . . 349
application-tracking . . . 350
association-timeout . . . 350
attack-threshold . . . 351
attacks (Exempt Rulebase) . . . 351
attacks (IPS Rulebase) . . . 352
attack-type (Anomaly) . . . 352
attack-type (Chain) . . . 353
attack-type (Signature) . . . 354
authentication . . . 357
authentication-algorithm . . . 358
authentication-method . . . 359
auto-re-enrollment . . . 360
automatic . . . 360
bind-interface . . . 361
block-command . . . 361
block-content-type . . . 362
block-mime . . . 362
bridge . . . 363

 Copyright © 2011, Juniper Networks, Inc.

c-timeout . . . 364
ca-identity . . . 364
ca-profile . . . 365
ca-profile-name . . . 366
cache . . . 366
cache-size . . . 367
call-flood . . . 367
category . . . 368
category (Security Logging) . . . 368
category (web filtering) . . . 369
certificate . . . 369
certificate-id . . . 370
chain . . . 371
challenge-password . . . 372
clear-threshold . . . 372
clients . . . 373
co-location . . . 373
code . . . 374
connection-flood . . . 374
connection-rate-threshold . . . 375
connections-limit . . . 375
container . . . 376
content-filtering (feature-profile) . . . 377
content-filtering (utm-policy) . . . 378
content-size . . . 379
content-size-limit . . . 380
context . . . 380
context (Application-Level DDoS) . . . 381
corrupt-file . . . 381
count (Custom Attack) . . . 382
count (Security Policies) . . . 382
crl . . . 383
custom-attack . . . 384
custom-attack-group . . . 388
custom-attacks . . . 388
custom-block-message . . . 389
custom-message (antivirus notification-options fallback-block/non-block) . . 389
custom-message (content-filter notification-options) . . . 390
custom-message-subject (antivirus notification-options fallback-block/non-block) . . . 390
custom-message-subject (antivirus notification-options virus-detection) 391
custom-message-subject (antivirus pattern-update email-notify) . . . 391
custom-objects . . . 392
custom-tag-string . . . 392
custom-url-category . . . 393
data-length . . . 393
datapath-debug . . . 394
dead-peer-detection . . . 395
decompress-layer . . . 395

decompress-layer-limit . . . 396
default (antivirus fallback-options) . . . 396
default (web-filtering fallback-settings) . . . 397
default-policy . . . 397
default-rule (Application Firewall) . . . 398
deny (Policy) . . . 398
deny (SIP) . . . 399
description (IDP Policy) . . . 399
description (Security Policies) . . . 400
destination (Destination NAT) . . . 401
destination (IP Headers in Signature Attack) . . . 402
destination-address (Destination NAT) . . . 403
destination-address (IDP Policy) . . . 403
destination-address (Security Policies) . . . 404
destination-address (Security Policies Flag) . . . 405
destination-address (Source NAT) . . . 406
destination-address (Static NAT) . . . 406
destination-except . . . 407
destination-ip . . . 407
destination-ip-based . . . 408
destination-nat . . . 408
destination-port (Destination NAT) . . . 409
destination-port (Signature Attack) . . . 409
destination-threshold . . . 410
detect-shellcode . . . 410
detector . . . 411
df-bit . . . 411
dh-group . . . 412
direction (Custom Attack) . . . 413
direction (Dynamic Attack Group) . . . 414
disable-call-id-hiding . . . 414
display-host (fallback-block) . . . 415
display-host (virus-detection) . . . 415
distinguished-name . . . 416
dns . . . 417
download-profile (ftp antivirus utm-profile) . . . 418
download-profile (ftp content-filtering utm-profile) . . . 418
download-timeout . . . 419
drop (gtp) . . . 420
drop (SCTP) . . . 424
dynamic . . . 426
dynamic-application . . . 426
dynamic-vpn . . . 427
dynamic-attack-group . . . 428
early-ageout . . . 429
email-notify . . . 429
enable-all-qmodules . . . 430
enable-packet-pool . . . 430
encryption . . . 431

Copyright © 2011, Juniper Networks, Inc.

encryption-algorithm 432
endpoint-registration-timeout 432
engine-not-ready 433
enrollment 434
establish-tunnels 435
event-rate 435
exception (antivirus mime-whitelist) 436
exception (content-filter block-mime) 436
exclude-context-values 437
expression 438
external-interface (IKE Gateway) 438
external-interface (Manual Security Association) 439
fallback-block 439
fallback-block (Sophos antivirus notification-options) 440
fallback-options (antivirus juniper-express-engine) 441
fallback-options (antivirus kaspersky-lab-engine) 442
fallback-options (antivirus sophos-engine) 443
fallback-settings (web-filtering surf-control-integrated) 443
fallback-settings (web-filtering websense-redirect) 444
fallback-settings (web-filtering juniper-local) 444
false-positives 445
family 446
feature-profile 447
filename-extension 450
filters 451
fin-no-ack 452
firewall-authentication (Policies) 452
firewall-authentication (Security) 453
first-update 454
first-update-interval 454
flood (ICMP) 455
flood (UDP) 456
flow (IDP) 457
flow (Security Flow) 458
force-upgrade 459
format (first use in Security Logging) 459
format (second use in Security Logging) 460
forwarding-options 460
forwarding-process 461
fragment 461
from 462
from-zone (IDP Policy) 462
from-zone (Security Policies) 463
ftp 465
ftp (content-filtering utm-policy) 466
functional-zone 467
gatekeeper 468
gateway (IKE) 469
gateway (Manual Security Association) 470

Copyright © 2011, Juniper Networks, Inc.

general-ikeid 470
global 471
gre-in 471
gre-out 472
group (Group VPN Server) 473
group-members 476
group-vpn 477
gtp 480
h323 483
handshake-timeout 484
header-length 484
hit-rate-threshold 485
high-watermark 486
host 486
host (Security Logging) 487
host (IDP Sensor Configuration) 487
host-address-base 488
host-inbound-traffic 488
hostname 489
http-profile (antivirus utm-policy) 489
http-profile (content-filtering utm-policy) 490
http-profile (web-filtering utm-policy) 490
icmp (Protocol Binding Custom Attack) 490
icmp (Security Screen) 491
icmp (Signature Attack) 492
identification (ICMP Headers in Signature Attack) 493
identification (IP Headers in Signature Attack) 493
idle-time 494
idp 495
idp-policy 502
ids-option 504
ignore-mem-overflow 505
ignore-regular-expression 506
ike (Group VPN Member) 507
ike (Group VPN Server) 508
ike (IPsec VPN) 509
ike (Security) 510
ike-policy 512
ike-user-type 512
imap-profile (antivirus utm-policy) 513
imap-profile (content-filtering utm-policy) 513
inactive-media-timeout (MGCP) 514
inactive-media-timeout (SCCP) 514
inactive-media-timeout (SIP) 515
inactivity-timeout 515
include-destination-address 516
inet 516
inet6 517
inet6 (IKE Gateway) 517

 Copyright © 2011, Juniper Networks, Inc.

inline-tap . . . 518
install-interval . . . 518
intelligent-prescreening . . . 519
interface (ARP Proxy) . . . 519
interface (Source NAT) . . . 520
interfaces . . . 521
interval (IDP) . . . 521
interval (IKE) . . . 522
interval (kaspersky-lab-engine) . . . 522
interval (juniper-express-engine) . . . 523
interval (sophons-engine) . . . 523
ip (Protocol Binding Custom Attack) . . . 524
ip (Security Screen) . . . 525
ip (Signature Attack) . . . 527
ip-action . . . 528
ip-action (Application-Level DDoS) . . . 529
ip-block . . . 529
ip-close . . . 530
ip-connection--rate-limit . . . 530
ip-flags . . . 531
ip-notify . . . 531
ips . . . 532
ipsec (Group VPN Server) . . . 533
ipsec-group-vpn (Group VPN) . . . 534
ipsec-policy . . . 534
ipsec-vpn (Flow) . . . 535
ipsec-vpn (Policies) . . . 535
ipsec-vpn (Dynamic VPNs) . . . 536
ip-sweep . . . 536
iso . . . 537
juniper-express-engine . . . 538
juniper-local . . . 539
kaspersky-lab-engine . . . 540
land . . . 541
large . . . 541
lifetime-kilobytes . . . 542
lifetime-seconds (Group VPN) . . . 542
lifetime-seconds (IKE) . . . 543
lifetime-seconds (IPsec) . . . 543
limit . . . 544
limit (SCTP) . . . 545
limit-session . . . 546
list (antivirus mime-whitelist) . . . 546
list (content-filter block-mime) . . . 547
local . . . 547
local-address . . . 548
local-certificate . . . 548
local-identity . . . 549
log (GTP) . . . 550

Copyright © 2011, Juniper Networks, Inc.

log (IDP) 551
log (IDP Policy) 551
log (SCTP) 552
log (Security Policies) 552
log (Security Logging) 553
log-attacks 554
log-errors 554
log-supercede-min 555
low-watermark 555
management 556
manual 557
match (Application Firewall) 558
match (Destination NAT) 558
match (IDP Policy) 559
match (rulebase-ddos) 560
match (Security Policies) 560
match (Source NAT) 561
match (Static NAT) 561
max-context-values 562
max-flow-mem 562
max-logs-operate 563
max–message–length 563
max-packet-mem 564
max-packet-memory 564
max-session-number 565
max-sessions 565
max-sessions (packet-log) 566
max-tcp-session-packet-memory 566
max-time-report 567
max-timers-poll-ticks 567
max-udp-session-packet-memory 568
maximize-idp-sessions 568
maximum-call-duration 569
maximum-message-length 569
mcc–mnc (gtp) 570
media-source-port-any 571
member (Group VPN) 572
member (IDP) 573
message-flood (H323) 574
message-flood (MGCP) 574
mgcp 575
mime-pattern 576
mime-whitelist 577
min–message–length 578
mode (Forwarding-Options) 579
mode (Policy) 580
mode (Security Logging) 580
mpls 581
msrpc 582

 Copyright © 2011, Juniper Networks, Inc.

mss . . . 583
nat . . . 584
nat-keepalive . . . 586
negate . . . 586
nested-application-identification . . . 587
nested-application-system-cache . . . 587
no-allow-icmp-without-flow . . . 587
no-anti-replay . . . 588
no-autoupdate . . . 588
no-enable-all-qmodules . . . 588
no-enable-packet-pool . . . 588
no-log-errors . . . 588
no-nat-traversal . . . 589
no-notify-mail-recipient (fallback-non-block) . . . 589
no-notify-mail-sender (fallback-block) . . . 590
no-notify-mail-sender (virus-detection) . . . 590
no-policy-lookup-cache . . . 590
no-reset-on-policy . . . 590
no-sequence-check . . . 591
no-syn-check . . . 591
no-uri-check . . . 592
no-syn-check-in-tunnel . . . 592
notification . . . 593
notification-options (antivirus juniper-express-engine) . . . 594
notification-options (antivirus kaspersky-lab-engine) . . . 595
notification-options (antivirus sophos-engine) . . . 596
notification-options (content-filtering) . . . 597
notify-mail-recipient (fallback-non-block) . . . 597
notify-mail-sender (antivirus fallback-block) . . . 598
notify-mail-sender (antivirus notification-options virus-detection) . . . 598
optimized . . . 599
option . . . 599
order . . . 600
out-of-resources . . . 600
over-limit . . . 601
overflow-pool . . . 602
packet-capture . . . 603
packet-filter . . . 604
packet-log (IDP Policy) . . . 605
pair-policy . . . 606
packet-log (Sensor Configuration) . . . 607
pass-through . . . 608
password-file . . . 609
pattern . . . 609
pattern-update (kaspersky-lab-engine) . . . 610
pattern-update (juniper-express-engine) . . . 610
pattern-update (sophos-engine) . . . 611
peer-certificate-type . . . 612
perfect-forward-secrecy . . . 612

Copyright © 2011, Juniper Networks, Inc.

performance . . . 613
permit (Persistent NAT) . . . 614
permit (Security Policies) . . . 615
permit-command . . . 616
persistent-nat . . . 616
ping-death . . . 617
pki . . . 618
policies . . . 620
policy (IKE) . . . 622
policy (IPsec) . . . 623
policy (Security) . . . 624
policy-lookup-cache . . . 625
policy-rematch . . . 625
pool (Destination NAT) . . . 626
pool (Source NAT) . . . 626
pool-utilization-alarm . . . 627
pop3-profile (antivirus utm-policy) . . . 627
pop3-profile (content-filtering utm-policy) . . . 628
port . . . 628
port (web filtering) . . . 629
port-randomization . . . 629
port-scan . . . 630
post-attack . . . 631
post-attack-timeout . . . 631
pptp . . . 632
pre-attack . . . 633
pre-filter-shellcode . . . 633
predefined-attack-groups . . . 634
predefined-attacks . . . 634
pre-shared-key . . . 635
process-ignore-s2c . . . 635
process-override . . . 636
process-port . . . 636
products . . . 637
profile (antispam sbl) . . . 637
profile (antivirus kaspersky-lab-engine) . . . 638
profile (antivirus juniper-express-engine) . . . 639
profile (Sophos Antivirus) . . . 640
profile (content-filtering) . . . 641
profile (gtp) . . . 642
profile (SCTP) . . . 645
profile (web-filtering surf-control-integrated) . . . 646
profile (web-filtering websense-redirect) . . . 647
profile (web-filtering juniper-local) . . . 648
proposal . . . 649
proposal-set (IKE) . . . 650
proposal-set (IPsec) . . . 651
proposals . . . 652
protect . . . 652

 Copyright © 2011, Juniper Networks, Inc.

protocol (IPsec) 653
protocol (Manual Security Association) 653
protocol (IP Headers in Signature Attack) 654
protocol (Signature Attack) 655
protocol-binding 658
protocol-command 659
protocol-name 659
protocols (Interface Host-Inbound Traffic) 660
protocols (Zone Host-Inbound Traffic) 662
proxy-arp 663
proxy-identity 663
raise-threshold 664
rate-limit 664
real 665
re-assembler 666
re-enroll-trigger-time-percentage 666
recommended 667
recommended-action 667
regexp 668
reject 668
reject-timeout 669
remote 669
remote-exceptions 670
remote-protected-resources 670
remove-r6 671
reset 671
reset-on-policy 672
respond-bad-spi 672
retain-hold-resource 673
revocation-check 673
route-change-timeout 674
routing-instance (Destination NAT) 674
routing-instance (Source NAT) 675
rpc 675
rsh 676
rst-invalidate-session 677
rst-sequence-check 677
rtsp 678
rule (Application Firewall) 679
rule (Application-Level DDoS Rulebase) 680
rule (Destination NAT) 681
rule (Exempt Rulebase) 682
rule (IPS Rulebase) 683
rule (Source NAT) 684
rule (Static NAT) 685
rulebase-ddos 686
rule-set (Application Firewall) 687
rule-set (Destination NAT) 688
rule-set (Source NAT) 689

Copyright © 2011, Juniper Networks, Inc.

rule-set (Static NAT) 690
rulebase-exempt 691
rulebase-ips 692
sbl 693
sbl-default-server 694
scan-mode 694
scan-options (antivirus juniper-express-engine) 695
scan-options (anti-virus kaspersky-lab-engine) 695
sccp 696
scheduler-name 697
scope (Chain Attack) 697
scope (Custom Attack) 698
screen (Security) 699
screen (Zones) 701
sctp 702
security-package 703
security-zone 704
sensor-configuration 705
seq-number-validated 706
server 707
server-connectivity 707
sessions 708
session-close 708
session-init 709
sessions-per-client 709
sequence-number (ICMP Headers in Signature Attack) 710
sequence-number (TCP Headers in Signature Attack) 710
server (Group VPN) 711
service (AppDDoS) 713
service (Anomaly Attack) 713
service (Dynamic Attack Group) 714
service (Security IPsec) 714
session-update-interval 715
severity (Custom Attack) 716
severity (Dynamic Attack Group) 717
severity (IPS Rulebase) 718
shellcode 719
signature 720
sip 724
smtp-profile (antispam utm-policy) 725
smtp-profile (antivirus utm-policy) 725
smtp-profile (content-filtering utm-policy) 725
sockets 726
sophos-engine 727
source (IP Headers in Signature Attack) 728
source (Source NAT) 729
source-address (Destination NAT) 730
source-address (IDP Policy) 731
source-address (IDP Sensor Configuration) 731

 Copyright © 2011, Juniper Networks, Inc.

source-address (Source NAT) 732
source-address (Security Policies) 732
source-except 733
source-interface 733
source-ip-based 734
source-nat 735
source-port 736
source-threshold 737
spam-action 737
spi 738
sql 739
ssh-known-hosts 740
ssl-inspection 741
start-log 741
start-time 742
static 742
static-nat 743
statistics 743
strict-syn-check 744
sunrpc 744
suppression 745
surf-control-integrated 746
sxl-retry 747
sxl-timeout 747
syn-ack-ack-proxy 748
syn-fin 748
syn-flood 749
syn-flood-protection-mode 749
syn-frag 750
system-services (Interface Host-Inbound Traffic) 751
system-services (Zone Host-Inbound Traffic) 753
t1-interval 754
t4-interval 755
talk 756
target 757
tcp (Protocol Binding Custom Attack) 758
tcp (Security Screen) 759
tcp (Signature Attack) 760
tcp-flags 762
tcp-initial-timeout 763
tcp-mss 764
tcp-no-flag 765
tcp-rst 765
tcp-session 766
tcp-sweep 767
terminal 767
test 768
tftp 769
then (Application Firewall) 770

Copyright © 2011, Juniper Networks, Inc.

then (Destination NAT) 770
then (IDP Policy) 771
then (rulebase-ddos) 772
then (Security Policies) 773
then (Source NAT) 774
then (Static NAT) 774
threshold 775
time-binding 775
time-binding-count 776
time-binding-period statement 777
timeout (GTP) 778
timeout (IDP Policy) 778
timeout (Security Screen) 779
timeout (antivirus fallback-options) 779
timeout (antivirus scan-options) 780
timeout (web-filtering surf-control-integrated cache) 780
timeout (web-filtering fallback-settings) 781
timeout (web-filtering websense-redirect profile) 781
to 782
to-zone 782
too-many-requests (antivirus fallback-options) 783
too-many-requests (web-filtering fallback-settings) 783
tos 784
total-length 785
total-memory 785
traceoptions (Application Firewall) 786
traceoptions (firewall-authentication) 787
traceoptions (H.323 ALG) 788
traceoptions (Flow) 789
traceoptions (firewall-authentication) 791
traceoptions (Group VPN) 792
traceoptions (IDP) 794
traceoptions (IKE) 796
traceoptions (IPsec) 798
traceoptions (MGCP ALG) 799
traceoptions (NAT) 800
traceoptions (datapath-debug) 802
traceoptions (PKI) 803
traceoptions (Policies) 805
traceoptions (SCCP ALG) 807
traceoptions (Screen) 808
traceoptions (SCTP) 810
traceoptions (Security) 811
traceoptions (SIP ALG) 813
traffic-options 814
transaction-timeout 814
trickling 815
trusted-ca 816
ttl 817

 Copyright © 2011, Juniper Networks, Inc.

tunable-name 817
tunable-value 818
tunnel 818
type (ICMP Headers in Signature Attack) 819
type (Dynamic Attack Group) 819
type (antivirus fallback-block) 820
type (antivirus feature-profile) 820
type (antivirus notification-options virus-detection) 821
type (content-filtering notification-options) 821
udp (Protocol Binding Custom Attack) 822
udp (Security Screen) 823
udp (Signature Attack) 824
udp-sweep 825
unknown-message (H.323 ALG) 826
unknown-message (MGCP ALG) 827
unknown-message (SCCP ALG) 828
unknown-message (SIP ALG) 829
upload-profile (ftp antivirus utm-profile) 830
upload-profile (ftp content-filtering utm-profile) 830
urgent-pointer 831
uri-check 831
url 832
url (kaspersky-lab-engine) 832
url (juniper-express-engine) 832
url (Sophos pattern-update) 833
url-blacklist 833
url-pattern 834
url-whitelist (antivirus) 834
url-whitelist (web-filtering) 835
user 835
user-at-hostname 836
utm 837
utm-policy 842
value-hit-rate-threshold 843
virus-detection 844
virus-detection (Sophos antivirus notification-options) 844
vpn 845
vpn-monitor 846
vpn-monitor-options 847
web-authentication 848
web-redirect 849
weight 850
wildcard 851
window-scale 851
window-size 852
winnuke 852
xauth 853
zones 854

Copyright © 2011, Juniper Networks, Inc.

Chapter 19 Services Hierarchy and Statements 857
Services Configuration Statement Hierarchy 857
address 859
application 860
application–identification 861
ca-profile 862
captive-portal 863
captive-portal (Unified Access Control policy) 864
download 865
dscp-rewrite 866
enable-heuristics 866
flow-monitoring 867
flow-monitoring version 9 867
flow-monitoring version 9 template 868
flow-server 869
flow-server version 9 870
infranet-controller 871
inline-jflow 872
interface 872
interval 873
max-checked-bytes 873
nested-application 874
nested-application-settings 875
no-application-identification 876
no-application-system-cache 876
option-refresh-rate 877
password 877
port 878
redirect-traffic 879
redirect-url 880
server-certificate-subject 881
signature 882
template-refresh-rate 883
test-only-mode 884
timeout 885
timeout-action 886
traceoptions (Application Identification Services) 887
traceoptions (Unified Access Control) 888
unified-access-control 889
Chapter 20 SNMP Hierarchy and Statements 891
SNMP Configuration Statement Hierarchy 891
authorization 895
client-list-name 896
Chapter 21 SMTP Hierarchy and Statements 897
SMTP Configuration Statement Hierarchy 897
flag 898
primary-server 899

 Copyright © 2011, Juniper Networks, Inc.

secondary-server 899
traceoptions 900

Chapter 22 **System Hierarchy and Statements 901**

System Configuration Statement Hierarchy 901
dhcpv6 914
dhcp-local-server (dhcpv6) 916
disable (dnssec) 919
dlv 919
dns 920
dnssec 921
firewall-authentication-service 921
forwarders 922
general-authentication-service 922
group (DHCP Local Server) 923
interface (DHCP Local Server) 924
interface-traceoptions (DHCP Local Server) 925
network-security 926
overrides (DHCP Local Server) 927
pki-local-certificate 928
propagate-settings 928
reconfigure (DHCP Local Server) 929
reverse ssh 930
reverse ssh port 930
reverse telnet 931
reverse telnet port 931
secure-domains 932
system-generated-certificate 932
traceoptions (DHCP Local Server) 933
traceoptions (dns) 935
traceoptions (General Authentication Service) 937
traceoptions (WAN Acceleration) 939
trusted-keys 940
wan-acceleration 941

Chapter 23 **WLAN Hierarchy and Statements 943**

[edit wlan] Configuration Statement Hierarchy 943
access-point 950
access-point-options 954
access-point-queues 955
arbitration-inter-frame-space 956
background-queue 956
beacon-interval 957
best-effort-queue 957
broadcast-multicast-rate-limit 958
channel 958
channel-management 959
cluster 960
cluster (access point) 963
console 963

country 964
default-cluster 965
disable-dot11d 966
dot1x 966
dot1x-supplicant 967
dtim-period 967
ethernet 968
external 969
fixed-multicast-rate 970
fragmentation-threshold 970
http-redirect 970
interfaces 971
logging-options 971
mac-authentication-type 972
management-vlan 972
maximum-stations 973
maximum-burst 973
maximum-contention-window 974
minimum-contention-window 974
mode 975
name 975
name-server 976
no-acknowledgement 976
no-auto-power-save 977
no-broadcast-ssid 977
no-short-guard-interval-supported 977
no-wifi-multimedia 978
ntp-server 978
protection 978
quality-of-service 979
radio 981
radio-off 983
radio-options 984
rts-threshold 985
security 986
space-time-block-coding 987
ssid 987
static 987
static-wep 988
station-mac-filter 989
station-queues 990
syslog-options 991
transmit-opportunity-limit 991
transmit-power 992
transmit-rate-sets 992
untagged-vlan 993
video-queue 993
virtual-access-point 994
vlan 995

Copyright © 2011, Juniper Networks, Inc.

voice-queue 996
wpa-enterprise 997
wpa-personal 998

Part 2 Operational Commands

Chapter 24 **Clear Commands 1001**

Clear Commands Overview 1001
clear chassis cluster control-plane statistics 1002
clear chassis cluster data-plane statistics 1003
clear chassis cluster failover-count 1004
clear chassis cluster ip-monitoring failure-count 1006
clear chassis cluster ip-monitoring failure-count ip-address 1007
clear chassis cluster statistics 1008
clear dhcpv6 server binding 1009
clear dhcpv6 server statistics 1010
clear esis adjacency 1011
clear esis statistics 1012
clear gtp tunnels 1013
clear interfaces statistics swfabx 1014
clear lacp statistics interfaces 1015
clear network-access requests pending 1016
clear network-access requests statistics 1017
clear network-access securid-node-secret-file 1018
clear security alg h323 counters 1019
clear security alg ike-esp-nat 1020
clear security alg mgcp calls 1021
clear security alg mgcp counters 1022
clear security alg sccp calls 1023
clear security alg sccp counters 1024
clear security alg sip calls 1025
clear security alg sip counters 1026
clear security application-firewall rule-set statistics 1027
clear security datapath-debug counters 1028
clear security dynamic-vpn all 1029
clear security dynamic-vpn user 1030
clear security firewall-authentication history 1031
clear security firewall-authentication history address 1032
clear security firewall-authentication history identifier 1033
clear security firewall-authentication users 1034
clear security firewall-authentication users address 1035
clear security firewall-authentication users identifier 1036
clear security flow ip-action family 1037
clear security flow session all 1038
clear security flow session application 1039
clear security flow session destination-port 1041
clear security flow session destination-prefix 1042
clear security flow session family 1044
clear security flow session interface 1045

clear security flow session protocol 1046
clear security flow session resource-manager 1048
clear security flow session session-identifier 1049
clear security flow session source-port 1050
clear security flow session source-prefix 1051
clear security gprs sctp counters 1052
clear security group-vpn member ike security-associations 1053
clear security group-vpn member ipsec security-associations 1054
clear security group-vpn member kek security-associations 1055
clear security group-vpn server 1056
clear security idp 1057
clear security idp application-identification application-system-cache 1058
clear security idp attack table 1059
clear security idp counters application-identification 1060
clear security idp counters dfa 1061
clear security idp counters flow 1062
clear security idp counters ips 1063
clear security idp counters log 1064
clear security idp counters packet 1065
clear security idp counters policy-manager 1066
clear security idp counters tcp-reassembler 1067
clear security idp ssl-inspection session-id-cache 1068
clear security ike respond-bad-spi-count 1069
clear security ike security-associations 1070
clear security ipsec security-associations 1072
clear security ipsec statistics 1074
clear security nat incoming-table 1075
clear security nat source persistent-nat-table 1076
clear security pki key-pair 1077
clear security pki local-certificate 1078
clear security policies statistics 1079
clear security screen statistics 1080
clear security screen statistics interface 1081
clear security screen statistics zone 1082
clear security utm anti-spam statistics 1083
clear security utm antivirus statistics 1084
clear security utm content-filtering statistics 1085
clear security utm session 1086
clear security utm web-filtering statistics 1087
clear services application-identification application-system-cache 1088
clear services application-identification counter 1089

Chapter 25 Request Commands 1091

Request Commands Overview 1091
request services application-identification download 1092
request services application-identification download status 1093
request services application-identification uninstall 1094
request chassis cluster failover node 1095
request chassis cluster failover reset 1096

 Copyright © 2011, Juniper Networks, Inc.

request modem wireless activate iota 1097
request modem wireless activate manual 1098
request modem wireless activate otasp 1100
request modem wireless gsm sim-unblock 1101
request modem wireless gsm sim-unlock 1102
request security datapath-debug capture start 1103
request security datapath-debug capture stop 1104
request security idp security-package download 1105
request security idp security-package install 1107
request security idp ssl-inspection key add 1109
request security idp ssl-inspection key delete 1111
request security pki ca-certificate verify 1113
request security pki local-certificate generate-self-signed 1114
request security pki local-certificate verify 1116
request security utm anti-virus juniper-express-engine 1117
request security utm anti-virus kaspersky-lab-engine 1118
request security utm anti-virus sophos-engine 1119
request system license update 1120
request system partition compact-flash 1121
request system services dhcp 1122
request system snapshot partition 1123
request system software add 1124
request system software in-service-upgrade 1125
request system software reboot 1127
request system software rollback 1128
request wan-acceleration login 1129
request wlan access-point firmware upgrade 1130
request wlan access-point firmware switch image 1131
request wlan access-point restart 1132

Chapter 26 Restart Commands 1133

Restart Commands Overview 1133
restart 1134

Chapter 27 Show Commands 1137

Show Commands Overview 1137
show bgp neighbor 1138
show configuration smtp 1142
show chassis cluster control-plane statistics 1143
show chassis cluster data-plane interfaces 1145
show chassis cluster data-plane statistics 1146
show chassis cluster interfaces 1148
show chassis cluster ip-monitoring status redundancy-group 1150
show chassis cluster statistics 1153
show chassis cluster status 1157
show chassis cluster ethernet-switching interfaces 1160
show chassis cluster ethernet-switching status 1161
show chassis fpc 1163
show chassis hardware 1166
show dhcpv6 server binding 1171

Copyright © 2011, Juniper Networks, Inc.

show dhcpv6 server statistics 1175
show esis adjacency 1177
show esis interface 1179
show esis statistics 1181
show ethernet-switching mac-learning-log 1183
show ethernet-switching table 1185
show gtp tunnels 1189
show igmp-snooping route 1190
show igmp-snooping vlans 1192
show interfaces 1194
show interfaces (Aggregated Ethernet) 1200
show interfaces flow-statistics 1212
show interfaces swfabx 1216
show lacp interfaces 1217
show lacp statistics interfaces 1221
show modem wireless interface 1222
show modem wireless interface firmware 1224
show modem wireless interface network 1226
show modem wireless interface rssi 1228
show network-access address-assignment pool 1229
show network-access requests pending 1230
show network-access requests statistics 1232
show network-access securid-node-secret-file 1233
show poe controller 1234
show poe interface 1235
show poe telemetries interface 1237
show schedulers 1239
show security alg h323 counters 1241
show security alg ike-esp-nat summary 1243
show security alg mgcp calls 1244
show security alg mgcp counters 1246
show security alg mgcp endpoints 1249
show security alg msrpc 1251
show security alg sccp calls 1252
show security alg sccp counters 1254
show security alg sip calls 1256
show security alg sip counters 1258
show security alg sip rate 1262
show security alg sip transactions 1264
show security alg status 1265
show security application-firewall rule-set 1267
show security application-tracking counters 1269
show security datapath-debug capture 1270
show security datapath-debug counter 1271
show security dynamic-policies 1272
show security dynamic-vpn client version 1277
show security dynamic-vpn users 1278
show security dynamic-vpn users terse 1279
show security firewall-authentication history 1280

 Copyright © 2011, Juniper Networks, Inc.

show security firewall-authentication history address 1282
show security firewall-authentication history identifier 1285
show security firewall-authentication users 1288
show security firewall-authentication users address 1290
show security firewall-authentication users identifier 1292
show security flow cp-session 1294
show security flow cp-session destination-port 1296
show security flow cp-session destination-prefix 1298
show security flow cp-session family 1300
show security flow cp-session protocol 1302
show security flow cp-session source-port 1304
show security flow cp-session source-prefix 1306
show security flow gate 1308
show security flow gate brief node 1312
show security flow gate destination-port 1318
show security flow gate destination-prefix 1321
show security flow gate family 1324
show security flow gate protocol 1326
show security flow gate source-port 1329
show security flow gate source-prefix 1332
show security flow gate summary node 1335
show security flow ip-action 1340
show security flow ip-action family 1341
show security flow session 1342
show security flow session application 1346
show security flow session brief node 1350
show security flow session destination-port 1354
show security flow session destination-prefix 1358
show security flow session extensive node 1362
show security flow session family 1367
show security flow session idp summary 1372
show security flow session interface 1374
show security flow session nat 1379
show security flow session protocol 1382
show security flow session resource-manager 1387
show security flow session session-identifier 1391
show security flow session source-port 1394
show security flow session source-prefix 1398
show security flow session summary family 1402
show security flow session summary node 1404
show security flow session tunnel 1409
show security flow statistics 1413
show security flow status 1414
show security gprs sctp counters 1415
show security group-vpn member ike security-associations 1416
show security group-vpn member ipsec security-associations 1420
show security group-vpn member kek security-associations 1423
show security group-vpn server ike security-associations 1426
show security group-vpn server ipsec security-associations 1430

Copyright © 2011, Juniper Networks, Inc.

show security group-vpn server kek security-associations 1434
show security group-vpn server registered-members 1438
show security idp active-policy 1440
show security idp application-ddos application 1441
show security idp application-identification application-system-cache 1443
show security idp attack table 1444
show security idp counters application-ddos 1445
show security idp counters application-identification 1448
show security idp counters dfa 1450
show security idp counters flow 1451
show security idp counters ips 1454
show security idp counters log 1456
show security idp counters packet 1459
show security idp counters packet-log 1462
show security idp counters policy-manager 1464
show security idp counters tcp-reassembler 1465
show security idp memory 1468
show security idp policies 1469
show security idp policy-templates 1470
show security idp predefined-attacks 1471
show security idp security-package-version 1473
show security idp ssl-inspection key 1474
show security idp ssl-inspection session-id-cache 1475
show security idp status 1476
show security idp status detail 1477
show security ike pre-shared-key 1478
show security ike security-associations 1479
show security ipsec next-hop-tunnels 1485
show security ipsec security-associations 1486
show security ipsec statistics 1492
show security match-policies 1495
show security monitoring fpc fpc-number 1499
show security monitoring performance session 1501
show security monitoring performance spu 1502
show security nat destination pool 1503
show security nat destination rule 1505
show security nat destination summary 1508
show security nat incoming-table 1510
show security nat interface-nat-ports 1512
show security nat source persistent-nat-table 1514
show security nat source pool 1517
show security nat source rule 1519
show security nat source summary 1522
show security nat static rule 1524
show security nat static-nat summary 1526
show security pki ca-certificate 1528
show security pki certificate-request 1532
show security pki crl 1534
show security pki local-certificate 1536

Copyright © 2011, Juniper Networks, Inc.

show security policies 1540
show security resource-manager group active 1544
show security resource-manager resource active 1546
show security resource-manager settings 1548
show security screen ids-option 1550
show security screen statistics 1553
show security softwires 1558
show security utm anti-spam statistics 1559
show security utm anti-spam status 1560
show security utm anti-virus statistics 1561
show security utm anti-virus status 1562
show security utm content-filtering statistics 1564
show security utm session 1565
show security utm status 1566
show security utm web-filtering statistics 1567
show security utm web-filtering status 1568
show security zones 1569
show security zones type 1571
show services accounting 1573
show services accounting aggregation 1574
show services accounting aggregation template 1575
show services accounting flow-detail 1576
show services application-identification application-system-cache 1577
show services application-identification counter 1579
show services application-identification version 1581
show services unified-access-control authentication-table 1582
show services unified-access-control policies 1583
show services unified-access-control status 1585
show system services dhcp client 1586
show system services dhcp relay-statistics 1589
show system snapshot media 1591
show system storage partitions 1592
show wan-acceleration status 1593
show wlan access-points 1594
show wlan diagnostics 1597

Part 3 Index

Index 1601

Copyright © 2011, Juniper Networks, Inc.

About This Guide

This preface provides the following guidelines for using the *Junos® OS CLI Reference*:

- J Series and SRX Series Documentation and Release Notes on page xxxix
- Objectives on page xl
- Audience on page xl
- Supported Routing Platforms on page xl
- Document Conventions on page xl
- Documentation Feedback on page xlii
- Requesting Technical Support on page xlii

J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see http://www.juniper.net/techpubs/software/junos-jseries/index-main.html .

For a list of related SRX Series documentation, see http://www.juniper.net/techpubs/hardware/srx-series-main.html .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Copyright © 2011, Juniper Networks, Inc.

Objectives

This reference documents command-line interface (CLI) statements and commands for J Series Services Routers and SRX Series Services Gateways running Junos OS. This reference provides the following information:

- Configuration hierarchies—Complete hierarchies of the configuration statements that you use to configure J Series and SRX Series devices. Hierarchies include all configuration statements—including the statements shared with the Junos OS—and highlight statements specific to the J Series and SRX Series devices in bold type.
- Configuration statements—Descriptions of the configuration statements that are unique to the J Series and SRX Series devices.
- Commands—Descriptions of the operational mode commands that you use to monitor and troubleshoot J Series and SRX Series operations.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J Series Services Router or an SRX Series Services Gateway running Junos OS. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running Junos OS.

Document Conventions

Table 1 on page xli defines the notice icons used in this guide.

Copyright © 2011, Juniper Networks, Inc.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xli defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1* | *string2* | *string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

Copyright © 2011, Juniper Networks, Inc.

or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

Copyright © 2011, Juniper Networks, Inc.

PART 1

Configuration Statements

- Access Hierarchy and Statements on page 3
- Accounting-Options Hierarchy on page 53
- Application Hierarchy and Statements on page 55
- Bridge-Domains Hierarchy and Statements on page 69
- Chassis Hierarchy and Statements on page 75
- Class-of-Service Hierarchy and Statements on page 103
- Event-Options Hierarchy on page 127
- Firewall Hierarchy and Statements on page 129
- Forwarding-Options Hierarchy and Statements on page 135
- Groups Hierarchy on page 141
- Interfaces Hierarchy and Statements on page 143
- Power Over Ethernet Hierarchy and Statements on page 195
- Policy-Options Hierarchy and Statements on page 203
- Protocols Hierarchy and Statements on page 207
- Routing-Instances Hierarchy on page 239
- Routing-Options Hierarchy on page 249
- Schedulers Hierarchy and Statements on page 257
- Security Hierarchy and Statements on page 273
- Services Hierarchy and Statements on page 857
- SNMP Hierarchy and Statements on page 891
- SMTP Hierarchy and Statements on page 897
- System Hierarchy and Statements on page 901
- WLAN Hierarchy and Statements on page 943

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 1

Access Hierarchy and Statements

This section includes the following topics:

- Access Configuration Statement Hierarchy on page 3

Access Configuration Statement Hierarchy

Use the statements in the **access** configuration hierarchy to configure access to the device and authentication methods, including address assignment and address pool, user and firewall authentication, a group profile, LDAP options and LDAP server configuration, an access profile, RADIUS options and RADIUS server configuration, and SecurID server configuration.

```
access {
  address-assignment {
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
      family {
        inet {
          dhcp-attributes {
            boot-file boot file name;
            boot-server boot server name;
            domain-name domain name;
            grace-period seconds;
            maximum-lease-time seconds;
            name-server address;
            netbios-node-type type;
            option dhcp option-identifier-code;
            option-match {
              option-82 {
                circuit-id match-value;
                remote-id match-value;
              }
            }
            router IPv4 address;
            server-identifier IP address;
            tftp-server server name;
            wins-server IPv4 address;
          }
          host hostname;
          network network address;
          range range-name {
```

Copyright © 2011, Juniper Networks, Inc.

```
                high upper-limit;
                low lower-limit;
            }
            xauth-attributes {
                primary-dns IP address;
                primary-wins IP address;
                secondary-dns IP address;
                secondary-wins IP address;
            }
        }
        inet6 {
            dhcp-attributes {
                dns-server IPv6-address;
                grace-period seconds;
                maximum-lease-time seconds;
                option dhcp-option-identifier-code;
                sip-server-address IPv6-address;
                sip-server-domain-name domain-name;
            }
            prefix IPv6-network-prefix;
            range range-name {
                high upper-limit;
                low lower-limit;
                prefix-length delegated-prefix-length;
            }
    link pool-name;
  }
}
address-pool pool-name {
  address address or address prefix;
  address-range {
    high upper-limit;
    low lower-limit;
    mask network-mask;
  }
  primary-dns IP address;
  primary-wins IP address;
  secondary-dns IP address;
  secondary-wins IP address;
}
domain {
  delimiter delimiter;
  map domain-map-name;
  parse-direction (left-to-right | right-to-left)
}
firewall-authentication {
  pass-through {
    default-profile profile-name;
    <ftp | http | telnet> {
      banner {
        fail string;
        login string;
        success string;
      }
    }
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
    traceoptions {
        file filename <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>
        flag flag;
    }
    web-authentication {
        banner {
            success string;
        }
        default-profile profile-name;
    }
}
group-profile profile-name {
    ppp {
        cell-overhead;
        encapsulated-overhead;
        framed-pool address-pool-name;
        idle-timeout seconds;
        interface-id interface-identifier;
        keepalive seconds;
        primary-dns IP address;
        primary-wins IP address;
        secondary-dns IP address;
        secondary-dns IP address;
    }
}
ldap-options {
    assemble {
        common-name common-name;
    }
    base-distinguished-name base-distinguished-name;
    revert-interval seconds;
    search {
        admin-search {
            distinguished-name distinguished-name;
            password password;
        }
        search-filter filter-name;
    }
}
ldap-server server-address {
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    source-address source-address;
    timeout seconds;
}
ppp-options {
    compliance 2486;
}
profile profile-name  {
    accounting {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        order [ radius ...]
        statistics;
```

```
    }
    address-assignment pool pool-name;
    authentication-order [ athentication-method1 authentication-method2 ... ]
    client client-name  {
      chap-secret  chap-secret;
      client-group [ group-names ];
      firewall-user {
        password password;
      }
      no-rfc2486;
      pap-password pap-password;
      x-auth client-ip-address;
      client-name-filter client-name {
        count number;
        domain-name domain-name;
        separator special-character;
      }
      ldap-options {
        assemble {
          common-name common-name;
        }
        base-distinguished-name base-distinguished-name;
        revert-interval seconds;
        search {
          admin-search {
            distinguished-name distinguished-name;
            password password;
          }
          search-filter filter-name;
        }
      }
      ldap-server server-address {
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        source-address source-address;
        timeout seconds;
      }
      radius-options {
        revert-interval seconds;
      }
      radius-server server-address {
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
      }
      session-options {
        client-group [group-names];
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
    radius-options {
        revert-interval seconds;
    }
    radius-server server-address {
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
    }
    securid-server {
        server-name configuration-file filepath;
    }
}
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Security Configuration Guide*
- *Junos OS System Basics Configuration Guide*

address-assignment

Syntax

```
address-assignment {
  neighbor-discovery-router-advertisement ndra-pool-name;
  pool pool-name {
    family {
      inet {
        dhcp-attributes {
          boot-file boot file name;
          boot-server boot server name;
          domain-name domain name;
          grace-period seconds;
          maximum-lease-time seconds;
          name-server address;
          netbios-node-type type;
          option dhcp option-identifier-code;
          option-match {
            option-82 {
              circuit-id match-value;
              remote-id match-value;
            }
          }
          router IPv4 address;
          server-identifier IP address;
          tftp-server server name;
          wins-server IPv4 address;
        }
        host hostname;
        network network address;
        range range-name {
          high upper-limit;
          low lower-limit;
        }
        xauth-attributes {
          primary-dns IP address;
          primary-wins IP address;
          secondary-dns IP address;
          secondary-wins IP address;
        }
      }
      inet6 {
        dhcp-attributes {
          dns-server IPv6-address;
          grace-period seconds;
          maximum-lease-time seconds;
          option dhcp-option-identifier-code;
          sip-server-address IPv6-address;
          sip-server-domain-name domain-name;
        }
        prefix IPv6-network-prefix;
        range range-name {
          high upper-limit;
          low lower-limit;
          prefix-length delegated-prefix-length;
```


Copyright © 2011, Juniper Networks, Inc.

```
            }
        link pool-name;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

address-pool

Syntax

```
address-pool pool-name {
   address address or address prefix;
   address-range {
      high upper-limit;
      low lower-limit;
      mask network-mask;
   }
   primary-dns IP address;
   primary-wins IP address;
   secondary-dns IP address;
   secondary-wins IP address;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Create an address-pool for L2TP clients.

Options

- **pool-name**—Name assigned to the address-pool.
- **address**—Configure subnet information for the address-pool.
- **address-range**—Defines the address range available for clients.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

admin-search

Syntax

```
admin-search {
   distinguished-name distinguished-name ;
   password password ;
}
```

Hierarchy Level

[edit access ldap-options search],
[edit access profile *profile-name* ldap-options search]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that a Lightweight Directory Access Protocol (LDAP) administrator search is performed. By default, the search is an anonymous search. To perform an administrator search, you must specify administrator credentials, which are used in the bind as part of performing the search.

Options

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

assemble

Syntax

```
assemble {
   common-name common-name;
}
```

Hierarchy Level

[edit access ldap-options],
[edit access profile *profile-name* ldap-options]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that a user's LDAP distinguished name (DN) is assembled through the use of a common name identifier, the username, and base distinguished name.

Options

common-name *common-name*—Common name identifier used as a prefix for the username during the assembly of the user's distinguished name. For example, **uid** specifies " user id," and **cn** specifies "common name."

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

authentication-order

Syntax authentication-order [*athentication-method1 authentication-method2 ...*]

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement modified in Release 9.1 of Junos OS.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the devices. For each login attempt, the software tries the authentication methods in order, from first to last.

Options

- **ldap**—Verify the client using LDAP.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.
- **securid**—Verify the client using SecurID authentication services.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

banner (FTP, HTTP, Telnet)

Syntax

```
banner {
   fail string ;
   login string ;
   success string ;
}
```

Hierarchy Level [edit access firewall-authentication pass-through (ftp | http | telnet)]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the banners that appear to users during the FTP, HTTP, and Telnet firewall authentication process. The banners appear during login, after successful authentication, and after failed authentication.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

banner (Web Authentication)

Syntax

```
banner {
  success string ;
}
```

Hierarchy Level [edit access firewall-authentication web-authentication]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the banners that appear to users during the Web authentication process. The banners appear during login, after successful authentication, and after failed authentication.

Options The remaining statement is explained separately.

Required Privilege Level
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

base-distinguished-name

Syntax base-distinguished-name ***base-distinguished-name***;

Hierarchy Level [edit access ldap-options],
[edit access profile ***profile-name*** ldap-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the base distinguished name (DN), which can be used in one of the following ways:

- If you are using the **assemble** statement so that the user's distinguished name is being assembled, the base distinguished name is appended to a username to generate the user's distinguished name. The resulting distinguished name is used in the LDAP bind call.
- If you are using the **search** statement so that the user's distinguished name is found by a search, the search is restricted to the subtree of the base distinguished name.

Options ***base-distinguished-name***—Series of basic properties that define the user. For example in the base distinguished name **o=juniper, c=us**, where **c** stands for country, and **o** for organization.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

client-group

Syntax client-group [*group-names*];

Hierarchy Level [edit access profile *profile-name* client *client-name*]
[edit access profile *profile-name session-options*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a list of client groups that the client belongs to. If the group list is not defined as part of the client profile, the client group configured at the **[edit access profile session-options]** hierarchy level is used.

Options ***group-names*** —Names of one or more groups the client belongs to, separated by spaces—for example **g1, g2, g3**. The total length of the group name string cannot exceed 256 characters.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

client-idle-timeout

Syntax client-idle-timeout *minutes*;

Hierarchy Level [edit access profile *profile-name* session-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user.

Options ***minutes*** —Number of minutes of idle time that elapse before the session is terminated.

Range: 10 through 255 minutes

Default: 10 minutes

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

client-name-filter

Syntax

```
client-name-filter client-name {
   count number;
   domain-name domain-name;
   separator special-character;
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define client-name-related restrictions. Clients whose names follow these restrictions are authenticated on the server.

Options ***client-name*** —Name of the client.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

client-session-timeout

Syntax client-session-timeout *minutes*;

Hierarchy Level [edit access profile *profile-name* session-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout).

Options ***minutes*** —Number of minutes after which user sessions are terminated.

Range: 1 through 10,000 minutes

Default: Off

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

configuration-file

Syntax *server-name* configuration-file *filepath*;

Hierarchy Level [edit access securid-server]

Release Information Statement introduced in Release 9.1 of Junos OS.

Description Specify the path of the SecurID server configuration file. The file is copied on the devices in some directory location—for example, **/var/db/securid/sdconf.rec**.

Options ***server-name***—Name of the SecurID authentication server.

filepath—Path of the SecurID server configuration file.

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

count

Syntax count *number*;

Hierarchy Level [edit access profile *profile-name* client-name-filter *client-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of characters to be stripped from a client name, from right to left, until the specified number of characters are deleted. The resulting name is sent to the authentication server.

Options ***number***—Number of characters to be stripped in a client name.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

default-profile

Syntax default-profile *profile-name*;

Hierarchy Level [edit access firewall-authentication pass-through]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the authentication profile to use if no profile is specified in a policy.

Options ***profile-name***—Name of the profile.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

dhcp-attributes (IPv4)

Syntax

```
dhcp-attributes {
  boot-file boot file name;
  boot-server boot server name;
  domain-name domain name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server address;
  netbios-node-type type;
  option dhcp option-identifier-code;
  option-match {
    option-82 {
      circuit-id match-value;
      remote-id match-value;
    }
  }
  router IPv4 address;
  server-identifier IP address;
  tftp-server server name;
  wins-server IPv4 address;
}
```

Hierarchy Level [edit access address-assignment pool pool-name family inet]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

dhcp-attributes (IPv6)

Syntax

```
dhcp-attributes {
   dns-server IPv6-address;
   grace-period seconds;
   maximum-lease-time seconds;
   option dhcp-option-identifier-code;
   sip-server-address IPv6-address;
   sip-server-domain-name domain-name;
}
```

Hierarchy Level

[edit access address-assignment pool pool-name family inet6]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Configure attributes for address pools that can be used by different clients.

Options

dns-server ***IPv6-address***—Specify a DNS server to which clients can send DNS queries.

grace-period ***seconds*** —Specify the grace period offered with the lease.

Range: 0 through 4,294,967,295 seconds

Default: 0 (no grace period)

maximum-lease-time ***seconds***—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

Range: 30 through 4,294,967,295 seconds

Default: 86,400 seconds (24 hours)

option ***dhcp-option-identifier-code***—Specify the DHCP option identifier code.

sip-server-address ***IPv6-address***—Specify the IPv6 address of the SIP outbound proxy server.

sip-server-domain-name ***domain-name***—Specify the domain name of the SIP outbound proxy server.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

distinguished-name

Syntax distinguished-name *distinguished-name*;

Hierarchy Level [edit access ldap-options search admin-search],
[edit access profile *profile-name* ldap-options search admin-search]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the distinguished name of an administrative user. The distinguished name is used in the bind for performing the LDAP search.

Options ***distinguished-name***—Set of properties that define the user. For example, **cn**=admin, **ou**=eng, **o**=juniper, **dc**=net.

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

domain-name

Syntax domain-name ***domain-name***;

Hierarchy Level [edit access profile ***profile-name*** client-name-filter ***client-name***]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a domain name that must be in a client's name during the authentication process.

Options ***domain-name***—Domain name that must be in a client name. The name must not exceed 128 characters.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

fail

Syntax fail *string*;

Hierarchy Level [edit access firewall-authentication pass-through default-profile *profile-name* (ftp | http | telnet) banner]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the banner that a client sees if the authentication process fails.

Options ***string***—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example, quotation marks (" ").

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

firewall-authentication

Syntax

```
firewall-authentication {
  pass-through {
    default-profile profile-name;
    <ftp | http | telnet> {
      banner {
        fail string;
        login string;
        success string;
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>
    flag flag;
  }
  web-authentication {
    banner {
      success string;
    }
    default-profile profile-name;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure default firewall authentication settings used by firewall authentication policies that restrict and permit access for firewall users to protected resources behind a firewall.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

firewall-user

Syntax

```
firewall-user {
   password password;
}
```

Hierarchy Level [edit access profile *profile-name* client *client-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a client as a firewall user and the associated password (encrypted).

Options **password** ***password***—Password used by the firewall user during local authentication.

Range: 1 through 128 characters

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ftp

Syntax

```
ftp {
   banner {
      fail string;
      login string;
      success string;
   }
}
```

Hierarchy Level [edit access firewall-authentication pass-through]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure banners for the FTP login prompt, successful authentication, and failed authentication.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

group-profile

Syntax

```
group-profile profile-name {
  ppp {
    cell-overhead;
    encapsulated-overhead;
    framed-pool address-pool-name;
    idle-timeout seconds;
    interface-id interface-identifier;
    keepalive seconds;
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-dns IP address;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure a group profile to define Point-to-Point Protocol (PPP) attributes. Any client referencing the configured group profile inherits all the group profile attributes.

Options

- **ppp**—Configure Point-to-Point Protocol (PPP) attributes.
- **cell-overhead**—Configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping.
- **framed-pool *pool-name***—Configure a framed-pool.
- **idle-timeout**—Configure the idle timeout for a user.
- **interface-id**—Configure the interface identifier.
- **keep-alive**—Configure the keepalive interval for an L2TP tunnel.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

http

Syntax

```
http {
  banner {
    fail string;
    login string;
    success string;
  }
}
```

Hierarchy Level [edit access firewall-authentication pass-through]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure banners for the HTTP login prompt, successful authentication, and failed authentication.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-address

Syntax ip-address *address*

Hierarchy Level [edit access profile *name* client *name* xauth]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Specify the ip-address for the client.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ldap-options

Syntax

```
ldap-options {
  assemble {
    common-name common-name;
  }
  base-distinguished-name base-distinguished-name;
  revert-interval seconds;
  search {
    admin-search {
      distinguished-name distinguished-name;
      password password;
    }
    search-filter filter-name;
  }
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure LDAP authentication options.

Options

The remaining options are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ldap-server

Syntax

```
ldap-server server-address {
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that the device use an LDAP server for authentication.

Options

server-address—Address of the LDAP authentication server.

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

link

Syntax

link *pool-name*;

Hierarchy Level

[edit access address-assignment pool]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Configure the name of the secondary address-assignment pool that is linked to a primary address-assignment pool. The secondary pool provides a backup pool for local address assignment.

Options

- *pool-name*—Name of the address assignment pool.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

login

Syntax login *string*;

Hierarchy Level [edit access firewall-authentication pass-through default-profile *profile-name* (ftp | http | telnet) banner]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the login banner for users using FTP, HTTP, and Telnet during the authentication process.

Options ***string***—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example quotation marks (" ").

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

name-server (address-assignment pool)

Syntax name-server *address*

Hierarchy Level [edit access address-assignment pool <name> family (inet | inet6) xauth-attributes]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Specify the DNS server IP address for an address-assignment pool.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

neighbor-discovery-router-advertisement

Syntax neighbor-discovery-router-advertisement *ndra-pool-name*;

Hierarchy Level [edit access address-assignment]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure the name of the address-assignment pool used to assign the router advertisement prefix.

Options
- *ndra-pool-name*—Name of the address assignment pool.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

network

Syntax network

Hierarchy Level [edit access address-assignment pool <name> family (inet | inet6)]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Specifies the IPv4 network address for the pool. This attribute is mandatory. For an IPv6 pool, you will set the IPv6 network prefix.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

pass-through

Syntax

```
pass-through {
   default-profile profile-name;
   <ftp | http | telnet> {
      banner {
         fail string;
         login string;
         success string;
      }
   }
}
```

Hierarchy Level [edit access firewall-authentication]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure pass-through firewall user authentication, when a host or user from one zone needs to access a protected resource in another zone. A user must use an FTP, Telnet, or HTTP client to access the IP address of the protected resource and get authenticated by the firewall. The device uses FTP, Telnet, and HTTP to collect username and password information. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication. After the user is authenticated, the firewall proxies the connection.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

password

Syntax password *password*;

Hierarchy Level [edit access ldap-options search admin-search],
[edit access profile *profile-name* ldap-options search admin-search]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the plain-text password for the administrative user. This password is used in the bind for performing the LDAP search.

Options ***password***—Administrative user password.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

pool (Address-Assignment Pools)

Syntax

```
pool pool-name {
  family {
    inet {
      dhcp-attributes {
        boot-file boot file name;
        boot-server boot server name;
        domain-name domain name;
        grace-period seconds;
        maximum-lease-time seconds;
        name-server address;
        netbios-node-type type;
        option dhcp option-identifier-code;
        option-match {
          option-82 {
            circuit-id match-value;
            remote-id match-value;
          }
        }
        router IPv4 address;
        server-identifier IP address;
        tftp-server server name;
        wins-server IPv4 address;
      }
      host hostname;
      network network address;
      range range-name {
        high upper-limit;
        low lower-limit;
      }
      xauth-attributes {
        primary-dns IP address;
        primary-wins IP address;
        secondary-dns IP address;
        secondary-wins IP address;
      }
    }
    inet6 {
      dhcp-attributes {
        dns-server IPv6-address;
        grace-period seconds;
        maximum-lease-time seconds;
        option dhcp-option-identifier-code;
        sip-server-address IPv6-address;
        sip-server-domain-name domain-name;
      }
      prefix IPv6-network-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length delegated-prefix-length;
      }
  link pool-name;
```

}

Hierarchy Level [edit access address-assignment]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure the name of an address assignment pool. The remaining statements are explained separately.

Options ***pool-name***—Name assigned to the address-assignment pool.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

port (LDAP)

Syntax port *port-number*;

Hierarchy Level [edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the port number on which to contact the LDAP server.

Options ***port-number***—Port number on which to contact the LDAP server.
Default: 389

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

port (RADIUS)

Syntax port *port-number*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure the port number on which to contact the RADIUS server.

Options ***port-number***—Port number on which to contact the RADIUS server.
Default: 1812 (as specified in RFC 2865)

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

prefix

Syntax prefix *IPv6-network prefix*;

Hierarchy Level [edit access address-assignment pool pool-name family inet6]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Specify the IPv6 prefix for the IPv6 address-assignment pool. This statement is mandatory for IPv6 address-assignment pools.

Options
- *IPv6-network-prefix*—IPv6 prefix.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

profile

Syntax

```
profile profile-name {
  accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order [ radius ...]
    statistics;
  }
  address-assignment pool pool-name;
  authentication-order [ athentication-method1 authentication-method2 ... ]
  client client-name {
    chap-secret chap-secret;
    client-group [ group-names ];
    firewall-user {
      password password;
    }
    no-rfc2486;
    pap-password pap-password;
    x-auth client-ip-address;
    client-name-filter client-name {
      count number;
      domain-name domain-name;
      separator special-character;
    }
    ldap-options {
      assemble {
        common-name common-name;
      }
      base-distinguished-name base-distinguished-name;
      revert-interval seconds;
      search {
        admin-search {
          distinguished-name distinguished-name;
          password password;
        }
        search-filter filter-name;
      }
    }
    ldap-server server-address {
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      source-address source-address;
      timeout seconds;
    }
    radius-options {
      revert-interval seconds;
    }
    radius-server server-address {
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
```


Copyright © 2011, Juniper Networks, Inc.

```
        source-address source-address;
        timeout seconds;
      }
      session-options {
        client-group [group-names];
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Create a profile containing a set of attributes that define device management access.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

radius-options

Syntax

```
radius-options {
  revert-interval seconds;
}
```

Hierarchy Level [edit access],
[edit access profile *profile-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure RADIUS options.

Options The remaining statement is explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

radius-server

Syntax

```
radius-server server-address {
   port port-number;
   retry attempts;
   routing-instance routing-instance-name;
   secret password;
   source-address source-address;
   timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Configure RADIUS for Layer 2 Tunneling Protocol (L2TP) or Point-to-Point Protocol (PPP) authentication.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

range

Syntax

```
range range-name {
   high upper-limit;
   low lower-limit;
   prefix-length delegated-prefix-length;
}
```

Hierarchy Level

[edit access address-assignment pool pool-name family inet6]
[edit access address-assignment pool pool-name family inet]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Configure an IP name range used within an address-assignment pool. For IPv4, you do not create a prefix-length.

Options

- *range-name*—Name of the range.
- **high** *upper-limit*—Upper limit of IPv6 address range.
- **low** *lower-limit*—Lower limit of IPv6 address range.
- **prefix-length** *delegated-prefix-length*—IPv6 delegated prefix length.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

retry (LDAP)

Syntax

retry *attempts*;

Hierarchy Level

[edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the number of retries that a device can attempt to contact an LDAP server.

Options

attempts—Number of retries that the device is allowed to attempt to contact an LDAP server.

Range: 1 through 10

Default: 3

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

retry (RADIUS)

Syntax retry *attempts*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the number of retries that a device can attempt to contact a RADIUS authentication server.

Options ***attempts***—Number of retries that the device is allowed to attempt to contact a RADIUS server.

Range: 1 through 10

Default: 3

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

revert-interval (LDAP)

Syntax revert-interval *seconds*;

Hierarchy Level [edit access ldap-options],
[edit access profile *profile-name* ldap-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the amount of time that elapses before the primary server is contacted if backup server is being used.

Options ***seconds***—Number of seconds that elapse before the primary server is contacted.

Range: 60 through 4,294,967,295 seconds

Default: 600 seconds

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

revert-interval (RADIUS)

Syntax revert-interval *seconds*;

Hierarchy Level [edit access radius-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the amount of time that elapses before the primary server is contacted if backup server is being used.

Options ***seconds***—Number of seconds that elapse before the primary server is contacted.

Range: 60 through 4,294,967,295 seconds

Default: 600 seconds

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

routing-instance (LDAP)

Syntax routing-instance *routing-instance-name*;

Hierarchy Level [edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the routing instance used to send LDAP packets to the LDAP server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables.

Options ***routing-instance-name***—Name of the routing instance.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

routing-instance (RADIUS)

Syntax

routing-instance *routing-instance-name*;

Hierarchy Level

[edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Configure the routing instance used to send RADIUS packets to the RADIUS server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables.

Options

routing-instance-name —Name of the routing instance.

Required Privilege Level

secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

search

Syntax

```
search {
  admin-search {
    distinguished-name distinguished-name;
    password password;
  }
  search-filter filter-name;
}
```

Hierarchy Level

[edit access ldap-options],
[edit access profile *profile-name* ldap-options]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that a search is used to get a user's LDAP distinguished name (DN). The search is performed based on the search filter and the part typed in by the user during authentication.

Options

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

search-filter

Syntax search-filter *filter-name*;

Hierarchy Level [edit access ldap-options search],
[edit access profile *profile-name* ldap-options search]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify that a search filter is used to find the user's LDAP distinguished name (DN). For example, a filter of **cn** specifies that the search matches a user whose common name is the username.

Options ***filter-name***—Name of the filter used to find the user's distinguished name.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

secret

Syntax secret *password*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the RADIUS secret password, which is shared between the router and the RADIUS server. The device uses this secret to encrypt the user's password that is sent to the RADIUS server.

Options ***password***—RADIUS secret. Maximum length is 256 characters.

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

securid-server

Syntax

```
securid-server {
   server-name configuration-file filepath;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Release 9.1 of Junos OS.

Description Configure SecurID server for SecurID authentication type.

Options The remaining statement is explained separately.

NOTE: You can configure only one SecurID server. SecurID challenges are not yet supported.

Required Privilege Level
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

separator

Syntax separator *special-character*;

Hierarchy Level [edit access profile *profile-name* client-name-filter *client-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a character to identify where stripping of characters occurs in a client name. Stripping removes characters to the right of each instance of the specified character, plus the character itself. The stripping begins with the rightmost separator character.

Use the **separator** statement with the **count** statement to determine which characters in a client name are stripped. If the specified number of separator characters (count) exceeds the actual number of separator characters in the client name, stripping stops at the last available separator character.

Options ***special-character***—Character used to identify where to start the stripping of characters in a client name.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

session-options

Syntax

```
session-options {
   client-group [group-names];
   client-idle-timeout minutes;
   client-session-timeout minutes;
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define options that control a user's session after successful authentication.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (LDAP)

Syntax source-address *source-address*;

Hierarchy Level [edit access ldap-server server-address],
[edit access profile *profile-name* ldap-server *server-address*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure a source address for each configured LDAP server. Each LDAP request sent to a LDAP server uses the specified source address.

Options ***source-address***—Valid IP address configured on one of the device interfaces.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (RADIUS)

Syntax source-address *source-address*;

Hierarchy Level [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

Options ***source-address*—Valid IP address configured on one of the device interfaces.**

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

success

Syntax

success *string*;

Hierarchy Level

[edit access firewall-authentication pass-through default-profile *name* (ftp | http | telnet) banner],
[edit access firewall-authentication web-authentication]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the banner (message) that users see when trying to connect using FTP, HTTP, or Telnet after successful authentication.

Options

string—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example, quotation marks (" ").

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

telnet

Syntax

```
telnet {
  banner {
    fail string;
    login string;
    success string;
  }
}
```

Hierarchy Level

[edit access firewall-authentication pass-through]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure banners for Telnet login prompt, successful authentication, and failed authentication.

Options

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

timeout (LDAP Server)

Syntax timeout *seconds*;

Hierarchy Level [edit access ldap-server *server-address*]
[edit access profile *profile-name* ldap-server *server-address*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the amount of time that the local device waits to receive a response from an LDAP server.

Options ***seconds***—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

timeout (RADIUS Server)

Syntax timeout *seconds*;

Hierarchy Level [edit access radius-server *server-address*]
[edit access profile *profile-name* radius-server *server-address*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure the amount of time that the local device waits to receive a response from a RADIUS server.

Options ***seconds***—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions

Syntax

```
traceoptions {
  file filename {
    files number;
    match regular-expression;
    size maximum-file-size;
    <world-readable | no-world-readable>;
  }
  flag flag;
}
```

Hierarchy Level [edit access firewall-authentication]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define Routing Engine firewall authentication tracing options.

Options

file ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files ***number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

size***maximum-file-size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the **trace-file** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.

- **all**—All tracing operations
- **authentication**—Trace authentication events
- **configuration**—Trace configuration events
- **setup**—Trace setup of firewall authentication service

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

xauth-attributes

Syntax

```
xauth-attributes {
   primary-dns IP address;
   primary-wins IP address;
   secondary-dns IP address;
   secondary-wins IP address;
}
```

Hierarchy Level
[edit access address-assignment pool <name> family (inet | inet6)]

Release Information
Statement introduced in Release 10.4 of Junos OS.

Description
Configure xauth attributes.

Options
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

web-authentication

Syntax

```
web-authentication {
   banner {
      success string
   }
   default-profile default-profile;
}
```

Hierarchy Level [edit access firewall-authentication]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify that users go through the Web authentication process. Users use HTTP to access an IP address on the **device** that is enabled for Web authentication. Users do not use HTTP to access the IP address of the protected resource in this case. Users are prompted for their username and password, which are verified by the device. Subsequent traffic from the user/host to the protected resource is allowed or denied based on the result of this authentication. This method of authentication differs from pass-through authentication in that users need to access the protected resource directly after accessing the Web authentication IP address and being authenticated.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

wins-server

Syntax wins-server *address*

Hierarchy Level [edit access address-assignment pool <name> family (inet | inet6) xauth-attributes]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Specify the wins-server IP address.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 2

Accounting-Options Hierarchy

This section contains the following topics:

- Accounting-Options Configuration Statement Hierarchy on page 53

Accounting-Options Configuration Statement Hierarchy

Use the statements in the **accounting-options** configuration hierarchy to collect and log data about basic system operations and services on the device.

```
accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name ;
    }
    file filename ;
    interval minutes ;
    source-classes {
      source-class-name ;
    }
  }
  file filename {
    archive-sites {
      site-name ;
    }
    files file-number ;
    nonpersistent;
    size bytes ;
    start-time time ;
    transfer-interval minutes ;
  }
  filter-profile profile-name {
    counters {
      counter name ;
    }
    file filename ;
    interval minutes ;
  }
  interface-profile profile-name {
    fields {
      field-name ;
    }
```

```
        file filename ;
        interval minutes ;
      }
      mib-profile profile-name {
        file filename ;
        interval minutes ;
        object-names {
          mib-object-name ;
        }
        operation operation-name ;
      }
      routing-engine-profile profile-name {
        fields {
          field-name ;
        }
        file filename ;
        interval minutes ;
      }
    }
```

Related Documentation

- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 3

Application Hierarchy and Statements

This section contains the following topics:

- Applications Configuration Statement Hierarchy on page 55

Applications Configuration Statement Hierarchy

Use the statements in the **applications** configuration hierarchy to configure applications properties and group applications objects for Domain Name Service (DNS), File Transfer Protocol (FTP), Media Gateway Control Protocol with Call Agent, Media Gateway Control Protocol with User Agent, Microsoft RPC, Point-to-Point Tunneling Protocol, ISDN connection control protocol (Q.931), Remote Access Service, RealAudio, UNIX remote shell services, Real-Time Streaming Protocol, Skinny Client Control Protocol, Session Initiation Protocol, Oracle SQLNET v2, Sun Microsystems RPC, the TALK program, and Trivial File Transfer Protocol.

```
applications {
  application application-name {
    application-protocol protocol-name ;
    destination-port port-number;
    icmp-code  value ;
    icmp-type  value ;
    inactivity-timeout  seconds ;
    protocol type;
    rpc-program-number  number ;
    source-port port-number;
    term term-name {
      alg application;
      destination-port port-number;
      icmp-code value;
      icmp-type value;
      inactivity-timeout seconds;
      protocol type;
      rpc-program-number number;
      source-port port-number;
      uuid hex-value;
    }
    uuid  hex-value;
  }
  application-set  application-set-name  {
    [application  application-name ];
```

```
    }
  }
```

Related Documentation

- *Junos OS Security Configuration Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Services Interfaces Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

alg

Syntax alg *application*;

Hierarchy Level [edit applications application *application-name* term *term-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define individual Application Layer Gateway (ALG).

Options *application* —Name of the application. The following protocols are supported:

- **dns**—Domain Name Service
- **ftp**—File Transfer Protocol
- **ignore**—Ignore application type
- **mgcp-ca**—Media Gateway Control Protocol with Call Agent
- **mgcp-ua**—MGCP with User Agent
- **ms-rpc**—Microsoft RPC
- **pptp**—Point-to-Point Tunneling Protocol
- **q931**—ISDN connection control protocol (Q.931)
- **ras**—Remote Access Service
- **realaudio**—RealAudio
- **rsh**—UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp**—Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **sqlnet-v2**—Oracle SQLNET v2
- **sun-rpc**—Sun Microsystems RPC
- **talk**—TALK program
- **tftp**—Trivial File Transfer Protocol

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-protocol

Syntax **application-protocol** ***protocol-name***;

Hierarchy Level [edit applications **application** ***application-name***]

Release Information Statement modified in Release 8.5 of Junos OS. **ike-esp-nat** option introduced in Release 10.2 of Junos OS.

Description Identify the application protocol name.

Options ***protocol-name*** —Name of the protocol. The following protocols are supported:

- **dns**—Domain Name Service
- **ftp**—File Transfer Protocol
- **ignore**—Ignore application type
- **ike-esp-nat**—IKE ESP NAT application protocol
- **mgcp-ca**—Media Gateway Control Protocol with Call Agent
- **mgcp-ua**—MGCP with User Agent
- **ms-rpc**—Microsoft RPC
- **pptp**—Point-to-Point Tunneling Protocol
- **q931**—ISDN connection control protocol (Q.931)
- **ras**—Remote Access Service
- **realaudio**—RealAudio
- **rsh**—UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp**—Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **sqlnet-v2**—Oracle SQLNET v2
- **sun-rpc**—Sun Microsystems RPC
- **talk**—TALK program
- **tftp**—Trivial File Transfer Protocol

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

destination-port

Syntax **destination-port** *port-number* ;

Hierarchy Level **[edit applications application** *application-name* **],**
[edit applications application *application-name* **term** *term-name* **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number.

Options *port-number* —Range of ports. You can use a numeric value or one of the text synonyms listed in Table 3 on page 60.

Table 3: Port Supported by Services Interfaces

Port Name	Corresponding Port Number
afs	1483
bgp	179
biff	512
bootpc	68
bootps	67
cmd	514
cvspserver	2401
dhcp	67
domain	53
eklogin	2105
ekshell	2106
excc	512
finger	79
ftp	21
ftp-data	20
http	80
https	443
ident	113
imap	143
kerberos-sec	88
klogin	543
kpasswd	761
krb-prop	754
krbupdate	760

Copyright © 2011, Juniper Networks, Inc.

Table 3: Port Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
kshell	544
ldap	389
ldp	646
login	513
mobileip-agent	434
mobilip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723
printer	515
radacct	1813
radius	1812
rip	520
rkinit	2108
smtp	25
snmp	161
snmp-trap	162

Copyright © 2011, Juniper Networks, Inc.

Table 3: Port Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs	49
tacacs-ds	65
talk	517
telnet	23
tftp	69
timed	525
who	513
xdmcp	177

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

icmp-code

Syntax **icmp-code** *value* ;

Hierarchy Level **[edit applications application** *application-name* **term** *term-name* **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the Internet Control Message Protocol (ICMP) code value.

Options *value* —ICMP code value, such as **host-unreachable** or **host-unreachable-for-tos**.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

icmp-type

Syntax **icmp-type** *value* ;

Hierarchy Level **[edit applications application** *application-name* **term** *term-name* **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the ICMP packet type value.

Options *value* —ICMP type value, such as **echo** or **echo-reply**.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inactivity-timeout

Syntax **inactivity-timeout** ***seconds*** **;**

Hierarchy Level **[edit applications application** ***application-name*** **term** ***term-name*** **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Inactivity timeout period, in seconds.

Options ***seconds*** —Length of time the application is inactive before it times out.
Default: 60 seconds

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

protocol

Syntax **protocol** *type* ;

Hierarchy Level [edit applications application *application-name*],
[edit applications application *application-name* term *term-name*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the networking protocol name or number.

Options ***protocol-name*** —Networking protocol name. The following text values are supported. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

- **ah**—IP Security Authentication Header
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload
- **gre**—Generic routing encapsulation
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP over IP
- **node**—Clear each session that uses the specified IP protocol on a specific node.
- **ospf**—Open Shortest Path First
- **pim**—Protocol Independent Multicast
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

NOTE: Internet Protocol version 6 (IPv6) is not supported as a network protocol in application definitions

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rpc-program-number

Syntax **rpc-program-number** *number* ;

Hierarchy Level **[edit applications application** *application-name* **term** *term-name* **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the remote procedure call (RPC) or Distributed Computing Environment (DCE) value.

Options ***number*** —RPC or DCE program value.

Range: 0 through 65,535

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-port

Syntax **source-port** *port-number* ;

Hierarchy Level [edit applications **application** *application-name*],
[edit applications application *application-name* **term** *term-name* **]**

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the source port identifier.

Options ***port-number*** —Identifier for the port. You can use a numeric value or one of the text synonyms listed in Table 3 on page 60.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

term

Syntax

```
term term-name {
  alg application ;
  destination-port port-number ;
  icmp-code value ;
  icmp-type value ;
  inactivity-timeout seconds ;
  protocol type ;
  rpc-program-number number ;
  source-port port-number ;
  uuid hex-value ;
}
```

Hierarchy Level [edit applications application *application-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define individual application protocols.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

uuid

Syntax uuid *hex-value* ;

Hierarchy Level [edit applications application *application-name* term *term-name*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the Universal Unique Identifier (UUID) for objects. DCE RPC services are mainly used by Microsoft applications. The ALG uses well-known TCP port 135 for port mapping services and uses the Universal Unique Identifier (UUID) instead of the program number to identify protocols. The main application-based DCE RPC is the Microsoft Exchange Protocol.

Support for stateful firewall and NAT services requires that you configure the DCE RPC port map ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

Options *hex-value* —Hexadecimal value.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

CHAPTER 4

Bridge-Domains Hierarchy and Statements

This section contains the following topics:

- Bridge-Domains Configuration Statement Hierarchy on page 69

Bridge-Domains Configuration Statement Hierarchy

Use the statements in the **bridge-domains** configuration hierarchy to configure a bridging domain that includes a set of logical ports that share the same flooding or broadcast characteristics.

```
bridge-domains bridge-domain-name {
   description description
   domain-type bridge;
   interface interface-name;
   vlan-id (none | number);
   vlan-id-list numbers;
   routing-interface routing-interface-name;
   bridge-options {
      interface interface-name;
      static-mac static-mac-address;
   }
}
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

bridge-domains

Syntax

```
bridge-domains bridge-domain-name {
   description description
   domain-type bridge;
   interface interface-name;
   vlan-id (none | number);
   vlan-id-list numbers;
   routing-interface routing-interface-name;
   bridge-options {
      interface interface-name;
      static-mac static-mac-address;
   }
}
```

Hierarchy Level

[edit]

Release Information

Statement modified in Release 9.5 of Junos OS.

Description

Configure a domain that includes a set of logical ports that share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Options

bridge-domain-name—Name of the bridge domain.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

bridge-options

Syntax

```
bridge-options {
  interface interface-name;
    static-mac static-mac-address;
  vlan-id number
}
```

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Configure Layer 2 learning and forwarding properties for a bridge domain.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

domain-type

Syntax domain-type bridge;

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Define the type of domain for a Layer 2 bridge domain.

Required Privilege Level routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

interface

Syntax interface *interface-name*;

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Specify the logical interfaces to include in the bridge domain.

Options ***interface-name***—Name of a logical interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*
- *Junos OS Interfaces Configuration Guide for Security Devices*

routing-interface

Syntax routing-interface *routing-interface-name*;

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Specify a routing interface to include in a bridge domain.

Options ***routing-interface-name***—Name of the integrated routing and bridging (IRB) interface to include in the bridge domain. The format of the interface name is **irb.*x***, where ***x*** is the unit number of the interface you configured at the **[edit interfaces irb]** hierarchy level.

NOTE: You can specify only one IRB interface for each bridge domain.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

static-mac

Syntax static-mac *mac-address*

Hierarchy Level [edit bridge-domains *bridge-domain-name* bridge-options interface *interface-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Configure a static MAC address for a logical interface in a bridge domain.

Options ***mac-address***—MAC address

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

vlan-id

Syntax vlan-id (none | *number*);

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Specify a VLAN identifier to include in the packets forwarded on the bridge domain.

Options ***number***—A valid VLAN identifier. If you configure multiple bridge domains with a valid VLAN identifier, you must specify a unique VLAN identifier for each domain.

none—Specify to enable shared VLAN learning.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

vlan-id-list

Syntax vlan-id-list *numbers*;

Hierarchy Level [edit bridge-domains *bridge-domain-name*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Specify multiple VLAN identifiers to create a bridge domain for each VLAN identifier.

Options ***numbers***—A list of valid VLAN identifiers. A bridge domain is created for each VLAN identifier in the list.

NOTE: If you specify a VLAN identifier list, you cannot configure an IRB interface in the bridge domain.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 5

Chassis Hierarchy and Statements

This section contains the following topics:

- Chassis Configuration Statement Hierarchy on page 75

Chassis Configuration Statement Hierarchy

Use the statements in the **chassis** configuration hierarchy to configure alarms, aggregated devices, clusters, the routing engine, and other chassis properties.

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
  }
  alarm {
    ds1 {
      ais (ignore | red | yellow);
      ylw (ignore | red | yellow);
    }
    ethernet {
      link-down (ignore | red | yellow);
    }
    integrated-services {
      failure (ignore | red | yellow);
    }
    management-ethernet {
      link-down (ignore | red | yellow);
    }
    serial {
      cts-absent (ignore | red | yellow);
      dcd-absent (ignore | red | yellow);
      dsr-absent (ignore | red | yellow);
      loss-of-rx-clock (ignore | red | yellow);
      loss-of-tx-clock (ignore | red | yellow);
    }
    services {
      hw-down (ignore | red | yellow);
      linkdown (ignore | red | yellow);
      pic-hold-reset (ignore | red | yellow);
      pic-reset (ignore | red | yellow);
```

Copyright © 2011, Juniper Networks, Inc.

```
        rx-errors (ignore | red | yellow);
        sw-down (ignore | red | yellow);
        tx-errors (ignore | red | yellow);
      }
      sonet {
        alarm-name  (ignore | red | yellow);
      }
      t3 {
        ais (ignore | red | yellow);
        exz (ignore | red | yellow);
        ferf (ignore | red | yellow);
        idle (ignore | red | yellow);
        lcv (ignore | red | yellow);
        lof (ignore | red | yellow);
        los (ignore | red | yellow);
        pll (ignore | red | yellow);
        ylw (ignore | red | yellow);
      }
    }
    cluster {
      control-link-recovery;
      control-ports {
        fpc slot-number port port-number;
      }
      heartbeat-interval milliseconds;
      heartbeat-threshold number;
      node node-number;
      redundancy-group group-number {
        gratuitous-arp-count number;
        hold-down-interval number;
        interface-monitor interface-name {
          weight number;
        }
        ip-monitoring {
          global-threshold number;
          global-weight number;
          retry-count count;
          retry-interval interval;
          family {
              inet {
                IP address {
                      weight number;
                      interface rethX.logical-unit-number secondary-ip-address IP address;
                    }
              }
          }
        }
        node node-number {
          priority priority-number;
        }
        preempt;
      }
      reth-count number;
      traceoptions {
        file filename {
          <files number>;
```


Copyright © 2011, Juniper Networks, Inc.

```
        <match regular-expression>;
        <size maximum-file-size>;
        <world-readable | no-world-readable>;
      }
      flag {
        all;
        configuration;
        routing-socket;
        snmp;
      }
    }
  }
  config-button {
    no-clear;
    no-rescue;
  }
  container-devices {
    device-count container-devices-number ;
  }
  craft-lockout;
  disable-power-management;
  fpc slot-number {
    offline;
    pic pic-number {
      aggregate-ports;
      atm-cell-relay-accumulation;
      atm-l2circuit-mode (cell | aal5 | trunk trunk );
      ce1 {
        e1 port-number {
          channel-group group-number timeslots slot-number ;
        }
      }
      ct3 {
        port port-number {
          t1 link-number {
            channel-group group-number timeslots slot-number ;
          }
        }
      }
      ds1{
        pic-mode (clear-channel | voice-ct1);
      }
      ethernet {
        pic-mode (enhanced-switching | routing | switching);
      }
      framing (sdh | sonet);
      idle-cell-format {
        itu-t;
        payload-pattern payload-pattern-byte ;
      }
      max-queues-per-interface (4 | 8);
      mlfr-uni-nni-bundles number ;
      no-concatenate;
      port port-number {
        framing (e3 | t3);
      }
```

```
            q-pic-large-buffer <(large-scale | small-scale)>;
            red-buffer-occupancy {
              weighted-averaged [ instant-usage-weight-exponent weight-value ];
            }
            shdsl {
              pic-mode (1-port-atm | 2-port-atm);
            }
            sparse-dlcis;
            traffic-manager {
              egress-shaping-overhead number ;
              ingress-shaping-overhead number ;
              mode ( egress-only | ingress-and-egress );
            }
            tunnel-queuing;
            tunnel-services {
              bandwidth (1g | 10g);
            }
            vtmapping (itu-t | klm);
          }
          power (off | on);
        }
        network-management {
          cluster-master;
        }
        pem {
          minimum number ;
        }
        redundancy {
          failover {
            on-disk-failure;
            on-loss-of-keepalives;
          }
          graceful-switchover;
          keepalive-time seconds ;
          routing-engine slot-number (backup | disabled | master);
        }
        routing-engine {
          on-disk-failure disk-failure-action (halt | reboot);
          bios {
            no-auto-upgrade;
            }
        }
      }
```

Related Documentation

- *Junos OS Security Configuration Guide*.
- *J Series Services Routers Hardware Guide*
- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS System Basics Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

cluster

Syntax

```
cluster {
  control-link-recovery;
  control-ports {
    fpc slot-number port port-number ;
  }
  heartbeat-interval milliseconds ;
  heartbeat-threshold number ;
  node node-number ;
  redundancy-group group-number {
    gratuitous-arp-count number ;
    hold-down-interval number ;
    interface-monitor interface-name {
      weight number ;
    }
    ip-monitoring {
      global-weight number ;
      global-threshold number;
      retry-count count;
      retry-interval interval;
      family {
          inet {
            IP address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP address;
              }
          }
      }
    }
    node node-number {
      priority priority-number ;
    }
    preempt;
  }
  reth-count number ;
  traceoptions {
    file filename {
      <files number >;
      <match regular-expression> ;
      <size maximum-file-size >;
      <world-readable | no-world-readable>;
    }
    flag {
      all;
      configuration;
      routing-socket;
      snmp;
    }
  }
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Configure a chassis cluster.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

control-link-recovery

Syntax control-link-recovery;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enable control link recovery to be done automatically by the system. After the control link recovers, the system checks whether it receives at least 30 consecutive heartbeats on the control link. This is to ensure that the control link is not flapping and is perfectly healthy. Once this criterion is met, the system issues an automatic reboot on the node that was disabled when the control link failed. When the disabled node reboots, the node rejoins the cluster. There is no need for any manual intervention.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

control-ports

Syntax

```
control-ports {
  fpc slot-number port port-number ;
}
```

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.2 of Junos OS. Support for dual control ports added in Release 10.0 of Junos OS.

Description Enable the specific control port of the Services Processing Card (SPC) for use as a control link for the chassis cluster. By default, all control ports are disabled. User needs to configure a minimum of one control port per chassis of the cluster. If user configures port 0 only, the Juniper Services Redundancy Protocol process (jsrpd) does not send control heartbeats on control link 1 and the counters it sends will show zeroes.

Options fpc *slot-number* —Flexible PIC Concentrator (FPC) slot number

NOTE: FPC slot range depends on platform. The maximum range of 0 through 23 applies to SRX5800 devices; for SRX5600 devices, the only applicable range is 0 through 11.

port *port-number* —Port number on which to configure the control port.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

framing

Syntax framing (e3 | t3);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* port *port-number*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Specifies the DS3 (t3) or E3 framing mode for the 1-Port Clear Channel DS3/E3 GPIM on an SRX650 device. By default, the GPIM port is configured in t3 mode.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

global-threshold

Syntax global-threshold *number* ;

Hierarchy Level [edit chassis cluster redundancy-group *group-number* ip-monitoring]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the failover value for all IP addresses monitored by the redundancy group. When IP addresses with a configured total weight in excess of the threshold have become unreachable, the weight of IP monitoring is deducted from the redundancy group threshold.

Options *number* —Value at which the IP monitoring weight will be applied against the redundancy group failover threshold.

Range: 0 through 255

Default: 0

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

global-weight

Syntax global-weight *number* ;

Hierarchy Level [edit chassis cluster redundancy-group *group-number* ip-monitoring]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the relative importance of all IP address monitored objects to the operation of the redundancy group. Every monitored IP address is assigned a weight. If the monitored address becomes unreachable, the weight of the object is deducted from the global-threshold of IP monitoring objects in its redundancy group. When the global-threshold reaches 0, the global-weight is deducted from the redundancy group. Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.

Options *number* —Combined weight assigned to all monitored IP addresses. A higher weight value indicates a greater importance.

Range: 0 through 255

Default: 255

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

gratuitous-arp-count

Syntax gratuitous-arp-count *number*;

Hierarchy Level [edit chassis cluster redundancy-group group-number]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the number of gratuitous Address Resolution Protocol (ARP) requests to send on an active interface after failover.

Options ***number***—Number of gratuitous ARP requests that a newly elected primary device in a chassis cluster sends out to announce its presence to the other network devices.

Range: 1 through 16

Default: 4

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

heartbeat-interval

Syntax heartbeat-interval *milliseconds*;

Hierarchy Level [edit **chassis cluster**]

Release Information Statement introduced in Release 9.0 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

Description Set the interval between the periodic signals broadcast to the devices in a chassis cluster to indicate that the active node is operational.

The **heartbeat-interval** option works in combination with the **heartbeat-threshold** option to define the wait time before failover is triggered in a chassis cluster. The default values of these options produce a wait time of 3 seconds. In a large configuration approaching full capacity on an SRX5600 or SRX5800 device, however, we recommend that you increase the failover wait time to 5 seconds. For a large configuration on an SRX3400 or SRX3600 device, increase the failover wait time to 8 seconds.

For example, a **heartbeat-threshold** of 3 and a **heartbeat-interval** of 1000 milliseconds result in a total wait of 3 seconds before failover is triggered. To increase this wait to 5 seconds, you could increase the **heartbeat-threshold**, the **heartbeat-interval**, or both. A **heartbeat-threshold** of 5 and a **heartbeat-interval** of 1000 milliseconds would yield a wait time of 5 seconds. Setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 1250 milliseconds would also yield a wait time of 5 seconds.

Options *milliseconds* —Time interval between any two heartbeat messages.

Range: 1000 through 2000 milliseconds

Default: 1000 milliseconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

heartbeat-threshold

Syntax heartbeat-threshold *number*;

Hierarchy Level [edit **chassis cluster**]

Release Information Statement introduced in Release 9.0 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

Description Set the number of consecutive missed heartbeat signals that a device in a chassis cluster must exceed to trigger failover of the active node.

The **heartbeat-threshold** option works in combination with the **heartbeat-interval** option to define the wait time before failover is triggered in a chassis cluster. The default values of these options produce a wait time of 3 seconds. In a large configuration approaching full capacity on an SRX5600 or SRX5800 device, however, we recommend that you increase the failover wait time to 5 seconds. For a large configuration on an SRX3400 or SRX3600 device, increase the failover wait time to 8 seconds.

For example, a **heartbeat-threshold** of 3 and a **heartbeat-interval** of 1000 milliseconds result in a total wait of 3 seconds before failover is triggered. To increase this wait to 5 seconds, you could increase the **heartbeat-threshold**, the **heartbeat-interval**, or both. A **heartbeat-threshold** of 5 and a **heartbeat-interval** of 1000 milliseconds would yield a wait time of 5 seconds. Setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 1250 milliseconds would also yield a wait time of 5 seconds.

Options *number* —Number of consecutive missed heartbeats.

Range: 3 through 8

Default: 3

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

hold-down-interval

Syntax hold-down-interval *number*;

Hierarchy Level [edit chassis cluster redundancy-group *group-number*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set the minimum interval to be allowed between back-to-back failovers for the specified redundancy group (affects manual failovers, as well as automatic failovers associated with monitoring failures).

For redundancy group 0, this setting prevents back-to-back failovers from occurring less than 5 minutes (300 seconds) apart. Note that a redundancy group 0 failover implies a Routing Engine failure.

For some configurations, such as ones with a large number of routes or logical interfaces, the default or specified interval for redundancy group 0 might not be sufficient. In such cases, the system automatically extends the dampening time in increments of 60 seconds until the system is ready for failover.

Options *number*—Number of seconds specified for the interval.

Range: For redundancy group 0, 300 through 1800 seconds; for redundancy group 1 through 128, 0 through 1800 seconds.

Default: For redundancy group 0, 300 seconds; for redundancy group 1 through 128, 1 second.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

interface

Syntax interface **reth***X.logical-unit-number* **secondary-ip-address** *IP–address*;

Hierarchy Level [edit chassis cluster redundancy-group *group-number* ip-monitoring family *family-name IP–address*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the redundant Ethernet interface, including its logical-unit-number, through which the monitored IP address must be reachable. The specified redundant Ethernet interface can be in any redundancy group. Likewise specify a secondary IP address to be used as a ping source for monitoring the IP address through the secondary node's redundant Ethernet interface link.

Options **reth***X.logical-unit-number*—Redundant Ethernet interface through which the monitored IP address must be reachable. You must specify the redundant Ethernet interface logical-unit-number. Note that you must also configure a secondary ping source IP address (see below).

Range: **reth0.***logical-unit-number* through **reth128.***logical-unit-number* (device dependent)

NOTE: If the redundant Ethernet interface belongs to a VPN routing and forwarding (VRF) routing instance type, then the IP Monitoring feature will not work.

secondary-ip-address *IP–address*—Specify the IP address that will be used as the source IP address of ping packets for IP monitoring from the secondary child link of the redundant Ethernet interface. An IP address for sourcing the ping packets on the primary link of the redundant Ethernet interface must be configured before you can configure secondary-ip-address. For legacy support reasons, monitoring on an IP address without identifying a redundant Ethernet interface and without configuring a secondary ping source IP address is permitted but not recommended.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

interface-monitor

Syntax

```
interface-monitor interface-name {
   weight number ;
}
```

Hierarchy Level

[edit **chassis cluster redundancy-group** *group-number*]

Release Information

Statement introduced in Release 9.0 of Junos OS.

Description

Specify a redundancy group interface to be monitored for failover and the relative weight of the interface.

Options

interface-name —Name of the physical interface to monitor.

The remaining statement is explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-monitoring

Syntax

```
ip-monitoring {
   global-threshold number;
   global-weight number;
   retry-count count;
   retry-interval interval;
   family {
         inet {
            IP-address {
                  weight number;
                  interface rethX.logical-unit-number secondary-ip-address IP-address;
               }
         }
   }
}
```

Hierarchy Level

[edit chassis cluster redundancy-group *group-number*]

Release Information

Statement updated in Release 10.1 of Junos OS.

Description

Specify a global IP address monitoring threshold and weight, and the interval between pings (**retry-interval**) and the number of consecutive ping failures (**retry-count**) permitted before an IP address is considered unreachable for all IP addresses monitored by the redundancy group. Also specify IP addresses, a monitoring weight, a redundant Ethernet interface number, and a secondary IP monitoring ping source for each IP address, for the redundancy group to monitor.

Options

family *family-name IP address*—The address to be continually monitored for reachability.

NOTE: All monitored object failures, including IP monitoring, are deducted from the redundancy group threshold priority. Other monitored objects include interface monitor, SPU monitor, cold-sync monitor, and NPC monitor (on supported platforms).

The remaining statement is explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

network-management

Syntax

```
network-management {
   cluster-master;
}
```

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Define parameters for network management. To manage an SRX Series Services Gateway cluster through a non-fxp0 interface, use this command to define the node as a virtual chassis in NSM. This command establishes a single DMI connection from the primary node to the NSM server. This connection is used to manage both nodes in the cluster. Note that the non-fxp0 interface (regardless of which node it is present on) is always controlled by the primary node in the cluster. The output of a *<get-system-information>* RPC returns a *<chassis-cluster>* tag in all SRX Series devices. When NSM receives this tag, it models SRX Series clusters as devices with autonomous control-planes.

Options **cluster-master**—Enable in-band management on the primary cluster node through NSM.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

node (Cluster)

Syntax node *node-number* ;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Identify the device in a chassis cluster. The node 0 device in the cluster has the chassis ID 1, and the node 1 device in the cluster has the chassis ID 2.

Options *node-number* —Cluster node number.

Range: 0 through 1

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

node (Redundancy-Group)

Syntax

```
node node-number {
  priority priority-number ;
}
```

Hierarchy Level [edit **chassis cluster redundancy-group** *group-number*]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Identify each cluster node in a redundancy group and set its relative priority for mastership.

Options *node-number* —Cluster node number, set with the **chassis cluster node** *node-number* statement.

The remaining statement is explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

pic-mode

Syntax pic-mode (enhanced-switching | routing | switching);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ethernet]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Set the mode to configure the uPIMs.

Options **enhanced-switching**—Enhanced switching mode of operation. Each port of the uPIMs can be configured for switching or routing mode.

NOTE: Only one **enhanced-switching** mode uPIM per chassis is supported currently.

routing—Routing mode of operation. All ports of the uPIMs are in routing mode. Routing mode is the default setting.

switching—Switching mode of operation. All ports of the uPIMs are in switching mode.

NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the **edit chassis fpc** command becomes **edit chassis node** *node-id* **fpc**.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pic-mode (Channel)

Syntax pic-mode (clear-channel);

Hierarchy Level [edit chassis fpc *slot-number* pic *pic-number* ds1]

Release Information Statement added in Release 10.2 of Junos OS.

Description Configure normal T1 mode or channelized T1 mode.

Options **clear-channel**—(default) Normal T1 mode.

ct1—Channelized T1 mode.

NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the edit chassis fpc command becomes edit chassis node *node-id* fpc.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

preempt

Syntax preempt;

Hierarchy Level [edit chassis cluster redundancy-group *group-number*]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Enable chassis cluster node preemption within a redundancy group. If **preempt** is added to a redundancy group configuration, the device with the higher priority in the group can initiate a failover to become master. By default, preemption is disabled.

Initiating a failover with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command overrides the priority settings and preemption.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

priority

Syntax **priority** *priority-number* ;

Hierarchy Level [edit **chassis cluster redundancy-group** *group-number* **node** *node-number*]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Define the priority of a node (device) in a redundancy group. Initiating a failover with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command overrides the priority settings.

Options *priority-number* —Priority value of the node. The eligible node with the highest priority is elected master.

Range: 1 through 254

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

redundancy-group

Syntax

```
redundancy-group group-number {
  gratuitous-arp-count number ;
  hold-down-interval number ;
  interface-monitor interface {
    weight number ;
  }
  ip-monitoring {
    global-weight number ;
    global-threshold number;
    retry-count count;
    retry-interval interval;
    family {
          inet {
            IP-address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP-address;
              }
          }
    }
  }
  node node-number {
    priority priority-number ;
  }
  preempt;
}
```

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Define a redundancy group. Except for redundancy group 0, a redundancy group is a logical interface consisting of two physical Ethernet interfaces, one on each chassis. One interface is active, and the other is on standby. When the active interface fails, the standby interface becomes active. The logical interface is called a redundant Ethernet interface (**reth**).

Redundancy group 0 consists of the two Routing Engines in the chassis cluster and controls which Routing Engine is primary. You must define redundancy group 0 in the chassis cluster configuration.

Options *group-number* —Redundancy group identification number.

Range: 0 through 128

NOTE: The maximum number of redundancy groups is equal to the number of redundant Ethernet interfaces that you configure.

The remaining statements are explained separately.

 Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

retry-count

Syntax
retry-count *count* ;

Hierarchy Level
[edit chassis cluster redundancy-group *group-number* ip-monitoring]

Release Information
Statement introduced in Release 10.1 of Junos OS.

Description
Specify the number of consecutive ping attempts that must fail before an IP address monitored by the redundancy group is declared unreachable. (See **retry-interval** for a related redundancy group IP address monitoring variable.)

Options
count—Number of consecutive ping attempt failures before a monitored IP address is declared unreachable.

Range: 1 through 15

Default: 5

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

retry-interval

Syntax retry-interval *interval* ;

Hierarchy Level [edit chassis cluster redundancy-group *group-number* ip-monitoring]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the ping packet send frequency (in seconds) for each IP address monitored by the redundancy group. (See **retry-count** for a related IP address monitoring configuration variable.)

Options *interval*—Pause time between each ping sent to each IP address monitored by the redundancy group.

Range: 1 to 30 seconds

Default: 1 second

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

reth-count

Syntax reth-count *number* ;

Hierarchy Level [edit **chassis cluster**]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the number of redundant Ethernet (**reth**) interfaces allowed in the chassis cluster. Note that the number of **reth** interfaces configured determines the number of redundancy groups that can be configured.

Options *number* —Number of redundant Ethernet interfaces allowed.

Range: 1 through 128

Default: 0

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag {
    all;
    configuration;
    routing-socket;
    snmp;
  }
}
```

Hierarchy Level [edit chassis cluster]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Define chassis cluster redundancy process tracing operations.

Options

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number* —(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0**, then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 0 KB through 1 GB

Default: 128 KB

Copyright © 2011, Juniper Networks, Inc.

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation or operations to perform on chassis cluster redundancy processes. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all the events
  - **configuration**—Trace configuration events
  - **routing-socket**—Trace logging of rtsock activity
  - **snmp**—Trace SNMP events

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tunnel-queuing

Syntax
tunnel-queuing;

Hierarchy Level
[edit chassis fpc *slot-number* pic *pic-number*]

Release Information
Statement modified in Release 9.0 of Junos OS.

Description
Enable class-of-service (CoS) queuing for generic routing encapsulation (GRE) and IP-IP tunnels.

NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the **edit chassis fpc** command becomes **edit chassis node** *node-id* **fpc**.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

weight

Syntax weight *number* ;

Hierarchy Level [edit chassis cluster **redundancy-group** *group-number* interface-monitor *interface*]
[edit chassis cluster **redundancy-group** *group-number* ip-monitoring *IP–address*]

Release Information Statement modified in Release 10.1 of Junos OS.

Description Specify the relative importance of the object to the operation of the redundancy group. This statement is primarily used with interface monitoring and IP address monitoring objects. The failure of an object—such as an interface—with a greater weight brings the group closer to failover. Every monitored object is assigned a weight.

- interface-monitor objects—If the object fails, its weight is deducted from the threshold of its redundancy group;
- ip-monitoring objects—If a monitored IP address becomes unreachable for any reason, the weight assigned to that monitored IP address is deducted from the redundancy group's global-threshold for IP address monitoring.

Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.

Options *number* —Weight assigned to the interface or monitored IP address. A higher weight value indicates a greater importance.

Range: 0 through 255

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 6

Class-of-Service Hierarchy and Statements

This section contains the following topics:

- Class-of-Service Configuration Statement Hierarchy on page 103

Class-of-Service Configuration Statement Hierarchy

Use the statements in the **class-of-service** configuration hierarchy to configure class-of-services (CoS) features.

```
class-of-service {
  adaptive-shapers {
    adaptive-shaper-name {
      trigger type shaping-rate (percent percent | rate );
    }
  }
  classifiers {
    type classifier-name {
      forwarding-class class-name {
        loss-priority (low | high) code-points [ alias | bits ];
      }
      import ( classifier-name | default);
    }
  }
  code-point-aliases {
    (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) {
      alias-name bits ;
    }
  }
  drop-profiles {
    profile-name {
      fill-level percentage drop-probability percentage ;
      interpolate {
        drop-probability value ;
        fill-level value ;
      }
    }
  }
  forwarding-classes {
    queue queue-number class-name priority (low | high);
```

```
}
forwarding-policy {
  class class-name {
    classification-override {
      forwarding-class class-name ;
    }
  }
  next-hop-map map-name {
    forwarding-class class-name {
      lsp-next-hop [ lsp-regular-expression ];
      next-hop [ next-hop-name ];
      non-lsp-next-hop [ lsp-regular-expression ];
    }
  }
}
fragmentation-maps {
  map-name {
    forwarding-class class-name {
      drop-timeout milliseconds ;
      fragment-threshold bytes ;
      multilink-class number ;
      no-fragmentation;
    }
  }
}
host-outbound-traffic {
  dscp-code-point value ;
  forwarding-class class-name ;
}
interfaces {
  interface-name {
    input-scheduler-map map-name ;
    input-shaping-rate rate ;
    scheduler-map map-name ;
    scheduler-map-chassis map-name ;
    shaping-rate rate ;
    unit logical-unit-number {
      adaptive-shaper adaptive-shaper-name ;
      classifiers {
        (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence)
        ( classifier-name | default);
      }
      forwarding-class class-name ;
      fragmentation-map map-name ;
      input-scheduler-map map-name ;
      input-shaping-rate (percent percentage | rate );
      input-traffic-control-profile profiler-name shared-instance instance-name ;
      loss-priority-maps {
        default;
        map-name ;
      }
      output-traffic-control-profile profile-name shared-instance instance-name ;
      rewrite-rules {
        dscp ( rewrite-name | default);
        dscp-ipv6 ( rewrite-name | default);
        exp ( rewrite-name | default) protocol protocol-types ;
```


Copyright © 2011, Juniper Networks, Inc.

```
            frame-relay-de ( rewrite-name | default);
            ieee-802.1 ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
            ieee-802.1ad ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
            inet-precedence ( rewrite-name | default);
          }
          scheduler-map map-name ;
          shaping-rate rate ;
          virtual-channel-group group-name ;
        }
      }
    }
    loss-priority-maps {
      frame-relay-de ( map-name | default) {
        loss-priority level code-points [ values ];
      }
    }
    rewrite-rules {
      type rewrite-name {
        forwarding-class class-name {
          loss-priority level code-point [ aliases ] [ 6-bit-patterns ];
        }
        import ( rewrite-name | default);
      }
    }
    scheduler-maps {
      map-name {
        forwarding-class class-name scheduler scheduler-name ;
      }
    }
    schedulers {
      scheduler-name {
        buffer-size (percent percentage | remainder percent | temporal microseconds );
        drop-profile-map {
          loss-priority (any | high | low | medium-high | medium-low);
          protocol (any | non-tcp | tcp);
        }
        priority (high | low | medium-high | medium-low | strict-high);
        shaping-rate (percent percent age | rate );
        transmit-rate (percent percentage | rate | remainder percent) <exact | rate-limit>;
      }
    }
    traceoptions {
      flag flag {
        all;
        asynch;
        hardware-database;
        init;
        parse;
        process;
        restart;
        route-socket;
        show;
        snmp;
        util;
      }
    }
```

```
    traffic-control-profiles profile-name {
      delay-buffer-rate (percent percent | rate );
      guaranteed-rate (percent percent | rate );
      scheduler-map map-name ;
      shaping-rate (percent percent | rate );
    }
    virtual-channel-groups {
      virtual-channel-group-name {
        virtual-channel-name {
          default;
          scheduler-map map-name ;
          shaping-rate (percent percent | rate );
        }
      }
    }
    virtual-channels {
      virtual-channel-name ;
    }
  }
```

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

adaptive-shaper

Syntax adaptive-shaper *adaptive-shaper-name*;

Hierarchy Level [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Assign an adaptive shaper to an interface.

Adaptive shapers enable bandwidth limits on Frame Relay interfaces when the device receives frames containing the backward explicit congestion notification (BECN) bit.

Options ***adaptive-shaper-name***—Name of the adaptive shaper.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **adaptive-shapers on page 107**
- *Junos OS Class of Service Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

adaptive-shapers

Syntax

```
adaptive-shapers {
  adaptive-shaper-name {
    trigger type shaping-rate (percent percentage | rate);
  }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define trigger types and associated rates. Adaptive shapers enable bandwidth limits on Frame Relay interfaces when the Services Router receives frames containing the backward explicit congestion notification (BECN) bit.

Options ***adaptive-shaper-name***—Name of the adaptive shaper.

The remaining statements are explained separately.

Required Privilege Level interface— view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **adaptive-shaper on page 106**
- *Junos OS Class of Service Configuration Guide for Security Devices*

classifiers

Syntax

```
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | ieee-802.1ad | inet-precedence) classifier-name {
    import (default | user-defined) ;
    forwarding-class class-name {
      loss-priority level code-points (alias | bits);
    }
  }
}
```

Hierarchy Level

[edit class-of-service]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure a user-defined behavior aggregate (BA) classifier.

Options

classifier-name—User-defined name for the classifier.

import (default | *user-defined*)—Specify the template to use to map any code points not explicitly mapped in this configuration. For example, if the classifier is of type **dscp** and you specify **import default**, code points you do not map in your configuration will use the predefined DSCP default mapping; if you specify **import mymap**, for example, code points not mapped in the forwarding-class configuration would use the mappings in a user-defined classifier named **mymap**.

forwarding-class *class-name*—Specify the name of the forwarding class. You can use the default forwarding class names or define new ones.

loss-priority *level*—Specify a loss priority for this forwarding class: **high**, **low**, **medium-high**, **medium-low**.

code-points (*alias* | *bits*)—Specify a code-point alias or the code points that map to this forwarding class.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

code-points (Forwarding Class)

Syntax code-points [*aliases*] [*6–bit-patterns*];

Hierarchy Level [edit class-of-service classifiers *type classifier-name* forwarding-class *class-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.

Options ***aliases***—Name of the DSCP alias.

6–bit patterns—Value of the code-point bits, in decimal form.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

default

Syntax default;

Hierarchy Level [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the default channel. You must configure one of the virtual channels in the group to be the default. Any traffic not explicitly directed to a virtual channel is transmitted by way of this default.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **scheduler-map (Virtual Channels) on page 119**
- **shaping-rate (Virtual Channels) on page 122**
- **virtual-channel-group on page 124**
- **virtual-channel-groups on page 125**
- **virtual-channels on page 123**
- *Junos OS Class of Service Configuration Guide for Security Devices*

frame-relay-de (Assigning to an Interface)

Syntax frame-relay-de (*name* | default);

Hierarchy Level [edit class-of-service interfaces *interface-name* unit *logical-unit-number* loss-priority-maps], [edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Assign the loss priority map or the rewrite rule to a logical interface.

Options **default**—Apply default loss priority map or default rewrite rule. The default loss priority map contains the following settings:

```
loss-priority low code-point 0;
loss-priority high code-point 1;
```

The default rewrite rule contains the following settings:

```
loss-priority low code-point 0;
loss-priority medium-low code-point 0;
loss-priority medium-high code-point 1;
loss-priority high code-point 1;
```

name—Name of loss priority map or rewrite rule to be applied.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

frame-relay-de (Defining Loss Priority)

Syntax

```
frame-relay-de map-name {
   loss-priority level code-poing (0 | 1);
}
```

Hierarchy Level

[edit class-of-service loss-priority-maps]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Define a Frame Relay discard-eligible bit loss-priority map.

Options

level—Level of loss priority to be applied based on the specified CoS values. The level can be **low**, **medium-low**, **medium-high**, or **high**.

map-name—Name of the loss-priority map.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

frame-relay-de (Defining Rewrite Rule)

Syntax

```
frame-relay-de rewrite-name {
  forwarding-class class-name {
    loss-priority level code-point (0 | 1);
  }
  import (default | rewrite-name);
}
```

Hierarchy Level [edit class-of-service rewrite-rules]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define a Frame Relay discard-eligible bit rewrite rule.

Options ***level***—Level of loss priority on which to base the rewrite rule. The loss priority level can be **low**, **medium-low**, **medium-high**, or **high**.

rewrite-name—Name of a rewrite-rules mapping configured at the **[edit class-of-service rewrite-rules]** hierarchy level.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Class of Service Configuration Guide for Security Devices*

forwarding-classes

Syntax

```
forwarding-classes {
  class class-name queue-num number;
}
```

Hierarchy Level [edit class-of-service forwarding-classes (class class-name *class-name* queue-num *number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure forwarding classes and assign queue numbers.

Options *class-name*—Displays the forwarding class name assigned to the internal queue number.

queue-number—Specifies the internal queue number to which a forwarding class is assigned.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

interface (class-of-service)

Syntax

```
interfaces {
  interface-name {
    input-scheduler-map map-name ;
    input-shaping-rate rate ;
    scheduler-map map-name ;
    scheduler-map-chassis map-name ;
    shaping-rate rate ;
    unit logical-unit-number {
      adaptive-shaper adaptive-shaper-name ;
      classifiers {
        (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence)
        ( classifier-name | default);
      }
      forwarding-class class-name ;
      fragmentation-map map-name ;
      input-schedular-map map-name ;
      input-shaping-rate (percent percentage | rate );
      input-traffic-control-profile profiler-name shared-instance instance-name ;
      loss-priority-maps {
        default;
        map-name ;
      }
      output-traffic-control-profile profile-name shared-instance instance-name ;
      rewrite-rules {
        dscp ( rewrite-name | default);
        dscp-ipv6 ( rewrite-name | default);
        exp ( rewrite-name | default) protocol protocol-types ;
        frame-relay-de ( rewrite-name | default);
        ieee-802.1 ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
        ieee-802.1ad ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
        inet-precedence ( rewrite-name | default);
      }
      scheduler-map map-name ;
      shaping-rate rate ;
      virtual-channel-group group-name ;
    }
  }
}
```

Hierarchy Level [edit class-of-service interface *interface-name* unit *number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Associate the class-of-service configuration elements with an interface.

Options interface *interface-name* unit *number*—The user-specified interface name and unit number.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

loss-priority (Frame Relay DE Bit Loss-Priority Map)

Syntax

loss-priority *level* code-points[*values*];

Hierarchy Level

[edit class-of-service loss-priority-maps frame-relay-de *map-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Map CoS values to a loss priority.

Options

level can be one of the following:

- **high**—Packet has high loss priority.
- **medium-high**—Packet has medium-high loss priority.
- **medium-low**—Packet has medium-low loss priority.
- **low**—Packet has low loss priority.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

loss-priority (Rewrite Rules)

Syntax loss-priority *level*;

Hierarchy Level [edit class-of-service rewrite-rules *type rewrite-name* forwarding-class *class-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a loss priority to which to apply a rewrite rule. The rewrite rule sets the code-point aliases and bit patterns for a specific forwarding class and packet loss priority (PLP). The inputs for the map are the forwarding class and the PLP. The output of the map is the code-point alias or bit pattern.

Options ***level*** can be one of the following:

- **high**—The rewrite rule applies to packets with high loss priority.
- **low**—The rewrite rule applies to packets with low loss priority.
- **medium-high**—The rewrite rule applies to packets with medium-high loss priority.
- **medium-low**—The rewrite rule applies to packets with medium-low loss priority.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Class of Service Configuration Guide for Security Devices*

loss-priority-maps (Assigning to an Interface)

Syntax

```
loss-priority-maps {
   frame-relay-de (map-name | default);
}
```

Hierarchy Level [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Assign the loss priority map to a logical interface.

Options **default**—Apply default loss priority map. The default map contains the following:

```
loss-priority low code-point 0;
loss-priority high code-point 1;
```

map-name—Name of loss priority map to be applied.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

loss-priority-maps (Defining)

Syntax

```
loss-priority-maps {
   frame-relay-de map-name {
      loss-priority level code-points [ values ];
   }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Map the loss priority of incoming packets based on CoS values.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

rewrite-rules (Definition)

Syntax

```
rewrite-rules {
   type rewrite-name{
      import (rewrite-name | default);
      forwarding-class class-name {
         loss-priority level code-point [ aliases ] [ 6–bit-patterns ];
      }
   }
}
```

Hierarchy Level

[edit class-of-service]

Release Information

Statement introduced in Release 8.5 of Junos OS. **ieee-802.1ad** option introduced in 9.2 of Junos OS.

Description

Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface.

Options

rewrite-name—Name of a **rewrite-rules** mapping.

type—Traffic type.

Values: **dscp**, **dscp-ipv6**, **exp**, **frame-relay-de** (J Series only), **ieee-802.1**, **ieee-802.1ad**, **inet-precedence**

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **rewrite-rules (Interfaces) on page 118**
- *Junos OS Class of Service Configuration Guide for Security Devices*

rewrite-rules (Interfaces)

Syntax

```
rewrite-rules {
   dscp (rewrite-name | default);
   dscp-ipv6 (rewrite-name | default);
   exp (rewrite-name | default) protocol protocol-types;
   exp-push-push-push default;
   exp-swap-push-push default;
   ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
   inet-precedence (rewrite-name | default);
}
```

Hierarchy Level

[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Associate a rewrite-rules configuration or default mapping with a specific interface.

Options

rewrite-name—Name of a **rewrite-rules** mapping configured at the **[edit class-of-service rewrite-rules]** hierarchy level.

default—The default mapping.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **rewrite-rules (Definition) on page 117**
- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

scheduler-map (Virtual Channels)

Syntax scheduler-map *map-name*;

Hierarchy Level [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Apply a scheduler map to this virtual channel.

Options ***map-name***—Name of the scheduler map.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **default on page 109**
- **shaping-rate (Virtual Channels) on page 122**
- **virtual-channel-group on page 124**
- **virtual-channel-groups on page 125**
- **virtual-channels on page 123**
- *Junos OS Class of Service Configuration Guide for Security Devices*

shaping-rate (Adaptive Shaping)

Syntax shaping-rate (percent *percentage* | *rate*);

Hierarchy Level [edit class-of-service adaptive-shapers *adaptive-shaper-name* trigger *type*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define the list of trigger types and associated rates.

Options **percent *percentage***—Shaping rate as a percentage of the available interface bandwidth.

Range: 0 through 100 percent

rate—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 3200 through 32,000,000,000 bps

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **trigger on page 122**
- *Junos OS Class of Service Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

shaping-rate (Applying to an Interface)

Syntax shaping-rate *rate*;

Hierarchy Level [edit class-of-service interfaces *interface-name*],
[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description For logical interfaces on which you configure packet scheduling, configure traffic shaping by specifying the amount of bandwidth to be allocated to the logical interface.

NOTE: The **shaping-rate** statement cannot be applied to a physical interface on J Series routing platforms.

Logical and physical interface traffic shaping is mutually exclusive. This means you can include the **shaping-rate** statement at the **[edit class-of-service interfaces interface *interface-name*]** hierarchy level or the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level, but not both.

Alternatively, you can configure a shaping rate for a logical interface and oversubscribe the physical interface by including the **shaping-rate** statement at the **[edit class-of-service traffic-control-profiles]** hierarchy level. With this configuration approach, you can independently control the delay-buffer rate. For more information on the delay-buffer rate, see the *Junos OS Class of Service Configuration Guide for Security Devices*.

Default If you do not include this statement at the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level, the default logical interface bandwidth is the average of unused bandwidth for the number of logical interfaces that require default bandwidth treatment. If you do not include this statement at the **[edit class-of-service interfaces interface *interface-name*]** hierarchy level, the default physical interface bandwidth is the average of unused bandwidth for the number of physical interfaces that require default bandwidth treatment.

Options ***rate***—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: For logical interfaces, 1000 through 32,000,000,000 bps.

For physical interfaces, 1000 through 160,000,000,000 bps.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Class of Service Configuration Guide for Security Devices*

shaping-rate (Virtual Channels)

Syntax shaping-rate (percent *percentage* | *rate*);

Hierarchy Level [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define the shaping rates to be associated with the virtual channel.

Options **percent** ***percentage***—Shaping rate as a percentage of the available interface bandwidth.

Range: 0 through 100 percent

rate—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 3200 through 32,000,000,000 bps

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **default on page 109**
- **scheduler-map (Virtual Channels) on page 119**
- **virtual-channel-group on page 124**
- **virtual-channel-groups on page 125**
- **virtual-channels on page 123**
- *Junos OS Class of Service Configuration Guide for Security Devices*

trigger

Syntax trigger *type* shaping-rate (percent *percentage* | *rate*);

Hierarchy Level [edit class-of-service adaptive-shapers *adaptive-shaper-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a trigger type and its associated rate.

Options ***type***—The type of trigger. Currently, the trigger type can be **becn** only.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **shaping-rate (Adaptive Shaping) on page 120**
- *Junos OS Class of Service Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

virtual-channels

Syntax

```
virtual-channels {
   virtual-channel-name;
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a list of virtual channels.

Each virtual channel has eight transmission queues.

Options ***virtual-channel-name***—Name of the virtual channel.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **default on page 109**
- **scheduler-map (Virtual Channels) on page 119**
- **shaping-rate (Virtual Channels) on page 122**
- **virtual-channel-group on page 124**
- **virtual-channel-groups on page 125**
- *Junos OS Class of Service Configuration Guide for Security Devices*

virtual-channel-group

Syntax virtual-channel-group *group-name*;

Hierarchy Level [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Assign a virtual channel group to a logical interface.

If you apply a virtual channel group to multiple logical interfaces, separate queues are created on each of the interfaces. The same virtual channel names are used on all the interfaces. You can specify the scheduler and shaping rates in the virtual channels in percentages so that you can apply the same virtual channel group to logical interfaces with different available bandwidths.

Options ***group-name***—Name of the virtual channel group.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **default on page 109**
- **scheduler-map (Virtual Channels) on page 119**
- **shaping-rate (Virtual Channels) on page 122**
- **virtual-channels on page 123**
- **virtual-channel-groups on page 125**
- *Junos OS Class of Service Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

virtual-channel-groups

Syntax

```
virtual-channel-groups {
  virtual-channel-group-name {
    virtual-channel-name {
      scheduler-map map-name;
      shaping-rate (percent percentage | rate);
      default;
    }
  }
}
```

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Associate a virtual channel with a scheduler map and a shaping rate. Virtual channels and virtual channel groups enable you to direct traffic into a virtual channel and apply bandwidth limits to the channel.

Options *group-name*—Name of the virtual channel group.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- **default on page 109**
- **scheduler-map (Virtual Channels) on page 119**
- **shaping-rate (Virtual Channels) on page 122**
- **virtual-channel-group on page 124**
- **virtual-channels on page 123**
- *Junos OS Class of Service Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 7

Event-Options Hierarchy

This section contains the following topics:

- Event-Options Configuration Statement Hierarchy on page 127

Event-Options Configuration Statement Hierarchy

Use the statements in the **event-options** configuration hierarchy to configure diagnostic event policies and actions associated with each policy.

```
event-options {
  destinations {
    destination-name {
      archive-sites {
        url password password ;
      }
      transfer-delay seconds ;
    }
  }
  event-script {
    file script-name ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  generate-event event-name {
    time-interval seconds ;
    time-of-day hh : mm : ss ;
  }
  policy policy-name {
    attributes-match {
      event1 . attribute-name equals event2 . attribute-name ;
      event .attribute-name matches regular-expression ;
      event1 . attribute-name starts-with event2 . attribute-name ;
    }
    events [ events ];
    then {
      event-script script-name .xml {
        arguments {
          name value ;
```

```
            }
            destination destination-name {
              retry-count number {
                retry-interval seconds ;
              }
              transfer-delay seconds ;
            }
            output-filename filename ;
            output-format (text | xml);
            user-name user-name ;
          }
          execute-commands {
            commands {
              "command";
            }
            destination destination-name {
              retry-count number {
                retry-interval seconds ;
              }
              transfer-delay seconds ;
            }
            output-file-name filename ;
            output-format (text | xml);
            user-name user-name ;
          }
          ignore;
          raise-trap;
          upload filename committed destination destination-name ;
          upload filename filename destination destination-name ;
        }
        within seconds not events [ events ];
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag ;
      }
    }
```

Related Documentation

- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Configuration and Operations Automation Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 8

Firewall Hierarchy and Statements

This section contains the following topics:

- Firewall Configuration Statement Hierarchy on page 129

Firewall Configuration Statement Hierarchy

Use the statements in the **firewall** configuration hierarchy to configure stateless firewall filters—also known as access control lists (ACLs)—on the device.

```
firewall {
  family family-name {
    dialer-filter filter-name {
      accounting-profile [ profile - name s];
      term term-name {
        from {
          match-conditions ;
        }
        then {
          action
          action-modifiers ;
          policer policer-name ;
          port-mirror;
          virtual-channel virtual-channel-name ;
        }
      }
    }
    filter filter-name {
      accounting-profile [ profile - names ];
      interface-specific;
      simple-filter filter-name {
        term term-name{
          from{
            match-conditions;
          }
          then{
            forwarding-class class-name ;
            loss-priority (high | low | medium) ;
          }
        }
      }
      term term-name {
```

```
            filter filter-name ;
            from {
              match-conditions ;
            }
            then {
              action ;
              action-modifiers ;
              policer policer-name ;
              port-mirror;
              virtual-channel virtual-channel-name ;
            }
          }
        }
        service-filter filter-name {
          term term-name {
            from {
              match-conditions ;
            }
            then {
              action ;
              action-modifiers ;
            }
          }
        }
        simple-filter filter-name {
          interface-specific;
          term term-name {
            from {
              match-conditions ;
            }
            then {
              action ;
              action-modifiers ;
            }
          }
        }
      }
      filter filter-name {
        accounting-profile [ profile-names ];
        interface-specific;
        term term-name {
          filter filter-name ;
          from {
            match-conditions ;
          }
          then {
            action ;
            action-modifiers ;
            virtual-channel virtual-channel-name ;
          }
        }
      }
      interface-set interface-set-name {
        [ interface-names ];
      }
      policer policer-name {
```

 Copyright © 2011, Juniper Networks, Inc.

```
        filter-specific;
        if-exceeding {
            bandwidth-limit rate ;
            bandwidth-percent number ;
            burst-size-limit bytes ;
        }
        logical-bandwidth-policer;
        logical-interface-policer;
        then {
            policer-action;
        }
    }
    three-color-policer policer-name {
        action {
            loss-priority high {
                then {
                    discard;
                }
            }
        }
        logical-interface-policer;
        single-rate {
            (color-aware | color-blind);
            committed-burst-size bytes ;
            committed-information-rate bps ;
            excess-burst-size bytes ;
        }
        two-rate {
            (color-aware | color-blind);
            committed-information-rate bps ;
            committed-burst-size bytes ;
            peak-information-rate bps ;
            peak-burst-size bytes ;
        }
    }
}
```

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Policy Framework Configuration Guide*

policer

Syntax

```
policer policer-name{
   logical-bandwidth-policer;
   if-exceeding {
      bandwidth-limit rate;
   burst-size-limit bytes;
   }
   then {
   policer-action;
   }
}
```

Hierarchy Level [edit firewall]

Release Information Command introduced in Release 9.5 of Junos OS.

Description Configure policer rate limits and actions. To activate a policer, you must include the policer action modifier in the **then** statement in a firewall filter term or on an interface.

Options ***policer-name***—Name of the policer to evaluate when packets are received on the interface.

Policer-action—One or more actions to take.

- **discard**—Always discard non conforming red packets.
- **forwarding-class *classname***—Specify the particular forwarding class.
- **loss-priority**—Set the loss priority to high or low.

then —Action to take on matching packets.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

simple-filter

Syntax

```
simple-filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      forwarding-class class-name;
      loss-priority (high | low | medium);
    }
  }
}
```

Hierarchy Level [edit firewall family *family-name* filter *filter-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Define a simple filter. Simple filters are recommended for metropolitan Ethernet applications.

Options

- **from**—Match packet fields to values. If the **from** option is not included, all packets are considered to match and the actions and action modifiers in the **then** statement are taken.
- **match-conditions**—One or more conditions to use to make a match.
- ***term-name***—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include space in the name, enclose it in quotation marks (“ ”).
- **then**—Actions to take on matching packets. If the then option is not included and a packet matches all the conditions in the from statement, the packet is accepted.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 9

Forwarding-Options Hierarchy and Statements

This section contains the following topics:

- Forwarding-Options Configuration Statement Hierarchy on page 135

Forwarding-Options Configuration Statement Hierarchy

Use the statements in the **forwarding-options** configuration hierarchy to configure forwarding options including protocol family, flow monitoring, accounting properties, load-balancing, port mirroring, traffic sampling, and packet capture.

```
forwarding-options {
  accounting group-name {
    output {
      aggregate-export-interval value ;
      cflowd [ hostnames ] {
        aggregation {
          autonomous-system;
          destination-prefix;
          protocol-port;
          source-destination-prefix {
            caida-compliant;
          }
          source-prefix;
        }
        autonomous-system-type;
        port;
        version;
      }
    }
  }
  family family-name {
    inet {
      filter (input | output);
    }
    inet6 {
      filter (input | output);
    }
    mpls {
      filter (input | output);
```

```
    }
  }
  hash-key {
    family {
      inet {
        layer-3;
        layer-4;
        session-id;
      }
      inet6 {
        layer-3;
        layer-4;
        session-id;
      }
      mpls {
        label-1;
        label-2;
        label-3;
        no-labels;
        payload {
          ip {
            layer-3-only;
            port-data {
              destination-lsb;
              destination-msb;
              source-lsb;
              source-msb;
            }
          }
        }
      }
    }
  }
  helpers {
    bootp {
      client-response-ttl value ;
      description text ;
      interface interface-name {
        broadcast;
        client-response-ttl number ;
        description description ;
        maximum-hop-count number ;
        minimum-wait-time seconds ;
        no-listen;
        server address ;
        vpn;
      }
      maximum-hop-count number ;
      minimum-wait-time seconds ;
      relay-agent-option;
      server address {
        routing-instance [ value ];
      }
      vpn;
    }
    domain {
```


Copyright © 2011, Juniper Networks, Inc.

```
        description text ;
        interface interface-name;
        server {
            address address ;
            routing-instance [ value ];
        }
    }
    port value {
        description text ;
        interface interface-name;
        server {
            address address ;
            routing-instance [ value ];
        }
    }
    tftp {
        description text ;
        interface interface-name;
        server {
            address address ;
            routing-instance [ value ];
        }
    }
    traceoptions {
        file filename {
            files number ;
            match regular-expression ;
            size maximum-file-size ;
            <world-readable | no-world-readable>;
        }
        flag {
            address;
            all;
            bootp;
            config;
            domain;
            ifdb;
            io;
            main;
            port;
            rtsock;
            tftp;
            trace;
            ui;
            util;
        }
        level level ;
    }
}
packet-capture {
    disable;
    file filename {
        <files number >;
        <size maximum-file-size >;
        <world-readable | no-world-readable>;
    }
```

```
    maximum-capture-size [ value ];
  }
  port-mirroring {
    family {
      inet {
        input {
          rate number ;
          run-length number ;
        }
        output {
          interface interface-name {
            next-hop {
              address ;
            }
          }
          no-filter-check;
        }
      }
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
    }
  }
  sampling {
    disable;
    family (inet | inet6 | mpls ) {
      disable;
      output {
        extension-service name;
        file;
        flow-server name {
          aggregation {
            source-destination;
          }
        }
      }
    }
    input {
      max-packets-per-second number;
      rate number ;
      run-length number ;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
    }
  }
}
```

Related Documentation

- *Junos OS Policy Framework Configuration Guide*
- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Services Interfaces Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

hash-key

Syntax

```
hash-key {
  family {
    inet {
      layer-3;
      layer-4;
      session-id;
    }
    inet6 {
      layer-3;
      layer-4;
      session-id;
    }
    mpls {
      label-1;
      label-2;
      label-3;
      no-labels;
      payload {
        ip {
          layer-3-only;
          port-data {
            destination-lsb;
            destination-msb;
            source-lsb;
            source-msb;
          }
        }
      }
    }
  }
}
```

Hierarchy Level **[edit forwarding-options]**

Release Information Statement modified in Release 10.2 of Junos OS.

Description Select which packet header data to use for per-flow load balancing.

Options

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.
- **mpls**—MPLS address family.
- **layer-3**—Incorporate Layer 3 data into the hash key.
- **layer-4**—Incorporate Layer 4 data into the hash key.
- **session-id**—Incorporate session ID data into the hash key (SRX3000 and SRX5000 lines only). The session ID data has higher precedence than the Layer 3 or 4 information.
- **label-1**—Incorporate the first MPLS label into the hash key.
- **label-2**—Incorporate the second MPLS label into the hash key.

- **label-3**—Incorporate the third MPLS label into the hash key.
- **no-labels**—Include no MPLS labels into the hash key.
- **payload**—Incorporate payload data into the hash key.
- **ip**—Include the IP address of the IPv4 or IPv6 payload into the hash key.
- **layer-3–only**—Include only Layer 3 IP information.
- **port-data**—Include the source and destination port field information.
- **source-msb**—Include the most significant byte of the source port.
- **source-lsb**—Include the least significant byte of the source port.
- **destination-msb**—Include the most significant byte of the destination port.
- **destinatione-lsb**—Include the least significant byte of the destination port.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Policy Framework Configuration Guide*

vpn

Syntax
vpn;

Hierarchy Level
[edit forwarding-options helpers bootp]

Release Information
Statement introduced in Release 9.0 of Junos OS.

Description
For Dynamic Host Configuration Protocol (DHCP) or BOOTP client request forwarding, enable virtual private network (VPN) encryption for a client request to pass through a VPN tunnel.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 10

Groups Hierarchy

This section contains the following topics:

- Groups Configuration Statement Hierarchy on page 141

Groups Configuration Statement Hierarchy

Use the statements in the **groups** configuration hierarchy to configure information that can be dynamically updated in various parts of the device configuration.

```
groups {
  group-name  {
    configuration-data ;
  }
}
```

Related Documentation

- *Junos OS CLI User Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 11

Interfaces Hierarchy and Statements

This section contains the following topics:

- Interfaces Configuration Statement Hierarchy on page 143

Interfaces Configuration Statement Hierarchy

Use the statements in the **interfaces** configuration hierarchy to configure interfaces on the device.

```
interfaces {
  interface-name {
    accounting-profile name ;
    aggregated-ether-options {
      lacp {
        (active | passive);
        periodic (fast | slow);
      }
      link-speed speed;
      minimum-links number;
    }
    atm-options {
      cell-bundle-size cells ;
      ilmi;
      linear-red-profiles profile-name {
        high-plp-max-threshold percent ;
        low-plp-max-threshold percent ;
        queue-depth cells high-plp-threshold percent low-plp-threshold percent ;
      }
      mpls {
        pop-all-labels {
          required-depth number ;
        }
      }
      pic-type (atm1 | atm2);
      plp-to-clp;
      promiscuous-mode {
        vpi vpi-identifier ;
      }
      scheduler-maps map-name {
        forwarding-class class-name {
          epd-threshold cells plp1 cells ;
```

```
            linear-red-profile profile-name ;
            priority (low | high);
            transmit-weight (cells number | percent number );
        }
        vc-cos-mode (alternate | strict);
    }
    vpi vpi-identifier {
        maximum-vcs maximum-vcs ;
        oam-liveness {
            down-count cells;
            up-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length |
            vbr peak rate sustained rate burst length );
            queue-length number ;
        }
    }
}
cellular-options {
    roaming-mode (home only | automatic)
    gsm-options {
        select-profile profile-name;
        profiles {
            profile-name {
                sip-user-id simple-ip-user-id;
                sip-password simple-ip-password;
                access-point-nameapn;
                authentication-method (pap | chap | none)
            }
        }
    }
}
clocking (external | internal);
dce;
description text ;
dialer-options {
    pool pool-identifier ;
    priority priority-number ;
}
disable;
dsl-options {
    loopback local;
    operating-mode mode ;
}
ds0-options {
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert data;
    loopback (payload | remote);
    start-end-flag (shared | filler);
```

 Copyright © 2011, Juniper Networks, Inc.

```
}
e1-options {
   bert-algorithm algorithm ;
   bert-error-rate rate ;
   bert-period seconds ;
   fcs (16 | 32);
   framing (g704 | g704-no-crc4 | unframed);
   idle-cycle-flag (flags | ones);
   invert data;
   loopback (local | remote);
   start-end-flag (shared | filler);
   timeslots time-slot-range;
}
e3-options {
   atm-encapsulation (direct | PLCP);
   bert-algorithm algorithm ;
   bert-error-rate rate ;
   bert-period seconds ;
   buildout feet;
   compatibility-mode (digital-link | kentrox | larscom) <subrate value >;
   fcs (16 | 32);
   framing (g.751 | g.832);
   idle-cycle-flag value ;
   loopback (local | remote);
   (payload-scrambler | no-payload-scrambler);
   start-end-flag value ;
   (unframed | no-unframed);
}
encapsulation type ;
ether-vpls-over-atm-llc;
es-options {
   backup-interface es- pim /0/ port ;
}
fabric-options {
   member-interfaces member-interface-name;
}
failure-options {
   [trigger-link-failure interface-name ];
}
fastether-options {
   (flow-control | no-flow-control);
   ingress-rate-limit rate ;
   (loopback | no-loopback);
   mpls {
      pop-all-labels {
         required-depth [ number ];
      }
   }
   redundant-parent interface-name;
   source-address-filter {
      mac-address ;
   }
   (source-filtering | no-source-filtering);
}
flexible-vlan-tagging;
framing (lan-phy | sdh | sonet | wan-phy);
```

```
gigether-options {
   802.3ad aex;
   (auto-negotiation <remote-fault
   (local-interface-online | local-interface-offline)> | no-auto-negotiation);
   (flow-control | no-flow-control);
   ignore-l3-incompletes;
   (loopback | no-loopback);
   mpls {
      pop-all-labels {
         required-depth [ number ];
      }
   }
   redundant-parent interface-name;
   source-address-filter {
      mac-address ;
   }
   (source-filtering | no-source-filtering);
   ethernet-switch-profile {
      ethernet-policer-profile {
         input-priority-map {
            ieee802.1p premium [ values ];
         }
         output-priority-map {
            classifier {
               premium {
                  forward-class class-name {
                     loss-priority (high | low);
                  }
               }
            }
         }
         policer cos-policer-name {
            aggregate {
               bandwidth-limit bps ;
               burst-size-limit bytes ;
            }
            premium {
               bandwidth-limit bps ;
               burst-size-limit bytes ;
            }
         }
      }
      (mac-learn-enable | no-mac-learn-enable);
      tag-protocol-id [ tpids ];
   }
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds ;
isdn-options {
   bchannel-allocation (ascending | descending) ;
   calling-number number ;
   incoming-called-number number <reject>;
   media-type (voice | data) ;
   network-type (cpe | network) ;
   pool pool-name <priority priority> ;
   spid1 spid-string ;
```


Copyright © 2011, Juniper Networks, Inc.

```
  spid2 spid-string ;
  static-tei-val value ;
  switch-type (att5e | etsi | ni1 | ntdms100 | ntt);
  t310 seconds ;
  tei-option (first-call | power-up);
}
keepalives <down-count number > <interval seconds > <up-count number >;
lmi {
  lmi-type (ansi | itu);
  n391dte number ;
  n392dce number ;
  n392dte number ;
  n393dce number ;
  n393dte number ;
  t391dte seconds ;
  t392dce seconds ;
}
mac mac-address ;
mlfr-uni-nni-bundle-options {
  acknowledge-retries number ;
  acknowledge-timer milliseconds ;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds ;
  fragment-threshold bytes ;
  hello-timer milliseconds ;
  link-layer-overhead percent ;
  lmi-type (ansi | itu);
  minimum-links number ;
  mrru bytes ;
  n391 number ;
  n392 number ;
  n393 number ;
  red-differential-delay milliseconds ;
  t391 seconds ;
  t392 seconds ;
  yellow-differential-delay milliseconds ;
}
modem-options {
  dialin (console | routable);
  init-command-string initialization-command-string ;
}
mtu bytes ;
multiservice-options {
  boot-command filename;
  (core-dump | no-core-dump);
  (syslog | no-syslog);
}
native-vlan-id vlan-id;
no-gratuitous-arp-request;
no-keepalives;
no-partition {
  interface-type type ;
}
partition partition-number {
  interface-type type ;
  oc-slice oc-slice-range ;
```

```
    timeslots time-slot-range ;
  }
  passive-monitor-mode;
  per-unit-scheduler;
  ppp-options {
    chap {
      access-profile name;
      default-chap-secret name ;
      local-name name;
      passive;
    }
    compression {
      acfc;
      pfc;
    }
    no-termination-request;
    lcp-restart-timer milliseconds ;
    ncp-restart-timer milliseconds ;
  }
  promiscuous-mode;
  redundant-ether-options {
    (flow-control | no-flow-control);
    lacp {
      (active | passive);
      periodic (fast | slow);
    }
    link-speed speed;
    (loopback | no-loopback);
    minimum-links number;
    redundancy-group number;
    source-address-filter mac-address;
    (source-filtering | no-source-filtering);
  }
  serial-options {
    clock-rate rate ;
    clocking-mode (dce | internal | loop);
    control-leads {
      control-signal (assert | de-assert | normal);
      cts (ignore | normal | require);
      dcd (ignore | normal | require);
      dsr (ignore | normal | require);
      dtr signal-handling-option ;
      ignore-all;
      indication (ignore | normal | require);
      rts (assert | de-assert | normal);
      tm (ignore | normal | require);
    }
    control-polarity (positive | negative);
    cts-polarity (positive | negative);
    dcd-polarity (positive | negative);
    dsr-polarity (positive | negative);
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (positive | negative);
    encoding (nrz | nrzi);
    indication-polarity (positive | negative);
    line-protocol protocol ;
```


Copyright © 2011, Juniper Networks, Inc.

```
    loopback mode;
    rts-polarity (positive | negative);
    tm-polarity (positive | negative);
    transmit-clock invert;
  }
  services-options {
    inactivity-timeout seconds ;
    open-timeout seconds ;
    syslog {
      host hostname {
        facility-override facility-name ;
        log-prefix prefix-number ;
        services priority-level ;
      }
    }
  }
  shdsl-options {
    annex (annex-a | annex-b);
    line-rate line-rate ;
    loopback (local | remote | payload);
    snr-margin {
      current margin ;
      snext margin ;
    }
  }
  t1-options {
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    buildout value ;
    byte-encoding (nx64 | nx56);
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flags (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots time-slot-range ;
  }
  t3-options {
    atm-encapsulation (direct | PLCP);
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    buildout feet;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink)
    <subrate value >;
    fcs (16 | 32);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value ;
    (long-buildout | no-long-buildout);
    (loop-timing | no-loop-timing);
    loopback (local | payload | remote);
```

```
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value ;
    (unframed | no-unframed);
  }
  threshold bytes ;
  traceoptions {
    flag flag < flag-modifier > <disable>;
  }
  (traps | no-traps);
  vdsl-options {
    vdsl-profile 17a;
  }
  unit logical-unit-number {
    accept-source-mac {
      mac-address mac-address ;
      policer {
        input policer-name ;
        output policer-name ;
      }
    }
    accounting-profile name ;
    allow-any-vci;
    atm-scheduler-map (default | map-name );
    backup-options {
      interface interface-name ;
    }
    bandwidth rate ;
    cell-bundle-size cells ;
    clear-dont-fragment-bit;
    compression {
      rtp {
        f-max-period number ;
        maximum-contexts number ;
        port {
          maximum port-number ;
          minimum port-number ;
        }
        queues [ queue-numbers ];
      }
    }
    compression-device interface-name;
    copy-tos-to-outer-ip-header;
    description text ;
    dialer-options {
      activation-delay seconds ;
      callback;
      callback-wait-period seconds ;
      deactivation-delay seconds ;
      dial-string [ dial-string-numbers ];
      idle-timeout seconds ;
      incoming-map (accept-all | caller caller-number );
      initial-route-check seconds ;
      load-interval seconds ;
      load-threshold percent ;
      pool pool-name ;
      redial-delay time ;
```

 Copyright © 2011, Juniper Networks, Inc.

```
  watch-list {
    [ routes ];
  }
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier ;
drop-timeout milliseconds ;
dynamic-call-admission-control {
  activation-priority number ;
  bearer-bandwidth-limit threshold ;
}
encapsulation;
(cisco-hdlc | frame-relay | multilink-frame-relay-uni-nni | ppp)
epd-threshold cells plp1 cells ;
f-max-period number ;
family {
  bridge {
    interface-mode {
      access vlan-id vlan-id |
      trunk {
        vlan-id-list vlan-list |
        vlan-rewrite translate from-vlan-id internal-vlan-id
      }
    }
  inet {
    address IP–address ;
    }
  }
  inet6 {
    address IP–address ;
    }
  }
}
fragment-threshold bytes ;
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap |
  swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number ;
  tag-protocol-id tpid;
  vlan-id number ;
}
interleave-fragments;
inverse-arp;
(keepalives | no-keepalives);
link-layer-overhead percent ;
minimum-links number ;
mrru bytes ;
multicast-dlci dlci-identifier ;
multicast-vci vpi-identifier.vci-identifier ;
multilink-max-classes number ;
multipoint number ;
multipoint;
oam-liveness {
  up-count cells ;
```

```
        down-count cells ;
      }
      oam-period (disable | seconds );
      output-vlan-map {
        (pop | pop-pop | pop-swap | push | push-push | swap |
        swap-push | swap-swap);
        inner-tag-protocol-id tpid;
        inner-vlan-id number ;
        tag-protocol-id tpid;
        vlan-id number ;
      }
      passive-monitor-mode;
      peer-unit unit-number ;
      plp-to-clp;
      point-to-point;
      ppp-options {
        chap {
          access-profile name ;
          default-chap-secret name ;
          local-name name ;
          passive;
        }
        compression {
          acfc;
          pfc;
        }
        lcp-restart-timer milliseconds ;
        loopback-clear-timer seconds ;
        ncp-restart-timer milliseconds ;
        no-termination-request;
        pap;
        access-profile name ;
        default-password password ;
        local-name name ;
        local-password password ;
        passive;
      }
    }
    pppoe-options {
      access-concentrator name ;
      auto-reconnect seconds ;
      service-name name ;
      underlying-interface interface-name ;
    }
    proxy-arp;
    service-domain (inside | outside);
    shaping{
      (cbr rate | rtvbr peak rate sustained rate burst length |
      vbr peak rate sustained rate burst length );
      queue-length number ;
    }
    short-sequence;
    three-color-policer {
      input policer-name ;
      output policer-name ;
    }
```


Copyright © 2011, Juniper Networks, Inc.

```
transmit-weight number ;
(traps | no-traps);
trunk-bandwidth rate ;
trunk-id number ;
tunnel {
  backup-destination address ;
  destination address ;
  key number ;
  routing-instance {
    destination routing-instance-name;
  }
  source source-address ;
  ttl number ;
}
vci vpi-identifier.vci-identifier ;
vpi vpi-identifier ;
vlan-id number ;
vlan-tagging native-vlan-id vlan-id;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id ;
family family {
  accounting {
    destination-class-usage;
    source-class-usage {
      direction ;
    }
  }
  address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address ;
    destination address ;
    destination-profile name ;
    eui-64;
    multipoint-destination address dlci dlci-identifier ;
    multipoint-destination address {
      epd-threshold cells ;
      inverse-arp;
      oam-liveness {
        up-count cells ;
        down-count cells ;
      }
      oam-period ( disable | seconds );
      shaping{
        (cbr rate | rtvbr peak rate sustained rate burst length |
        vbr peak rate sustained rate burst length );
        queue-length number ;
      }
      vci vpi-identifier.vci-identifier ;
    }
    preferred;
    primary;
    vrrp-group group-number {
      (accept-data | no-accept-data):
      advertise-interval seconds ;
      authentication-type authentication ;
      authentication-key key ;
      fast-interval milliseconds;
```

```
        (preempt | no-preempt) {
          hold-time seconds ;
        }
        priority number ;
        track {
          interface interface-name {
            priority-cost priority ;
            bandwidth-threshold bits-per-second {
              priority-cost priority ;
            }
          }
          priority-hold-time seconds ;
        }
        virtual-address [ addresses ];
      }
      web-authentication {
        http;
      }
    }
    bundle interface-name ;
    dhcp {
      client-identifier (ascii ascii | hexadecimal hexadecimal);
      lease-time seconds;
      retransmission-attempt number;
      retransmission-interval seconds;
      server-address ip-address;
      update-server;
      vendor-id vendor-id;
    }
    dialer filter-name;
    filter {
      group filter-group-number;
      input filter-name;
      input-list {
        [filter-names];
      }
      output filter-name ;
      output-list {
        [filter-names];
      }
    }
    keep-address-and-control;
    mtu bytes ;
    multicast-only;
    next-hop-tunnel gateway-address ipsec-vpn vpn-name;
    no-redirects;
    policer {
      arp policer-template-name;
      input policer-template-name;
      output policer-template-name;
    }
    primary;
    proxy inet-address address ;
    receive-options-packets;
    receive-ttl-exceeded;
    remote (inet-address address | mac-address address);
```


Copyright © 2011, Juniper Networks, Inc.

```
            rpf-check <fail-filter filter-name> {
              <mode loose>;
            }
            sampling {
              direction ;
            }
            service {
              input {
                service-set service-set-name <service-filter filter-name >;
                post-service-filter filter-name ;
              }
              output {
                service-set service-set-name <service-filter filter-name >;
              }
            }
            simple-filter{
              input filter-name;
            }
            (translate-discard-eligible | no-translate-discard-eligible);
            (translate-fecn-and-becn | no-translate-fecn-and-becn);
            unnumbered-address {
              interface-name ;
              destination destination-address ;
              destination-profile profile-name ;
              preferred-source-address interface-name ;
            }
          }
        }
        traceoptions {
          flag flag <disable>;
        }
      }
      traceoptions {
        file filename <files number > <match regular-expression >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag <disable>;
      }
```

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*
- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Interfaces Configuration Guide*
- *Junos OS Services Interfaces Configuration Guide*

access-point-name

Syntax **access-point-name** *apn*;

Hierarchy Level [**edit interfaces** *interface-name* **cellular-options gsm-options profiles** *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the access point name (APN) provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

Options ***apn***—Access point name.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

activation-priority

Syntax activation-priority *priority*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* **dynamic-call-admission-control**]

Release Information Statement introduced in Release 8.2 of Junos OS.

Description This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550 media gateway module. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure the dynamic call admission control (dynamic CAC) activation priority value.

Options ***priority***—The activation priority at which the interface is used for providing call bandwidth. The interface with the highest activation priority value is the primary link for providing call bandwidth. If the primary link becomes unavailable, the TGM550 switches over to the next active interface with the highest activation priority value, and so on.

Range: 0 through 255

Default: 50

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

annex

Syntax annex *annex-type*

Hierarchy Level [edit interfaces *interfaces-name* shdsl-options]

Release Information Command introduced in Release 10.0 of Junos OS.

Description Select an annex type that suits your requirements for configuring G.SHDSL interface.

Options
- Annex A
- Annex B
- Annex F
- Annex G

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

authentication-method

Syntax **authentication-method (pap | chap | none);**

Hierarchy Level **[edit interfaces *interface-name* cellular-options gsm-options profiles *profile-name*]**

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Specify the authentication method for connection to a Global System for Mobile Communications (GSM) cellular network.

Options **pap**—Password Authentication Protocol.

chap—Challenge Handshake Authentication Protocol.

none—No authentication method is used.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

bandwidth

Syntax bandwidth <*value*>;

Hierarchy Level [edit interfaces *interface-name* radio—router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This option controls the weight of the current (vs. maximum) data rate (value 0–100).

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

bearer-bandwidth-limit

Syntax bearer-bandwidth-limit *kilobits-per-second*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* **dynamic-call-admission-control**]

Release Information Statement introduced in Release 8.2 of Junos OS.

Description This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure the bearer bandwidth limit (BBL). The BBL is used for dynamic call admission control (dynamic CAC) to provide enhanced control over WAN bandwidth.

Options ***kilobits-per-second***—The bearer bandwidth limit to be reported to a TGM550, in kilobits per second (Kbps).

Range: 0 through 9999 Kbps

Default: –1 (dynamic CAC is not enabled on the interface)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

bundle

Syntax bundle;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family mlppp]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Specify the logical interface name the link joins.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

cbr rate

Syntax cbr rate;

Hierarchy Level [edit interfaces interface-name atm-options vpi vpi-identifier shaping]

Release Information Command introduced in Release 9.5 of Junos OS.

Description For ATM encapsulation only, define a constant bit rate bandwidth utilization in the traffic-shaping profile.

Options CBR Value - Constant bandwidth utilization (range: 33,000 through 1,199,920)

CDVT - Cell delay variation tolerance in microseconds (range: 1 through 9999)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

cellular-options

Syntax

```
cellular-options {
  roaming-mode (home only | automatic)
  gsm-options {
    select-profile profile-name;
    profiles {
      profile-name {
        sip-user-id simple-ip-user-id;
        sip-password simple-ip-password;
        access-point-name apn;
        authentication-method (pap | chap | none);
      }
    }
  }
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure options for connecting a 3G wireless modem interface to a cellular network.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

client-identifier

Syntax client-identifier (ascii *ascii* | hexadecimal *hexadecimal*);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify an ASCII or hexadecimal identifier for the Dynamic Host Configuration Protocol (DHCP) client. The DHCP server identifies a client by a client-identifier value.

Options ascii *ascii* —Identifier consisting of ASCII characters.

hexadecimal *hexadecimal* —Identifier consisting of hexadecimal characters.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

compression-device

Syntax compression-device *name*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before Release 7.4 of Junos OS.

Description For J Series routers with PPP over Ethernet interfaces, configure the name of the access concentrator (AC).

Options ***name***—Name of the AC.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

credit

Syntax
```
credit {
interval;
}
```

Hierarchy Level [edit interfaces *interface-name* radio—router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This parameter controls credit-based scheduling parameters and includes an interval option to set the grant rate interval to a value between 1–60 seconds.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

dhcp

Syntax

```
dhcp {
   client-identifier (ascii ascii | hexadecimal hexadecimal );
   lease-time seconds ;
   retransmission-attempt number ;
   retransmission-interval seconds ;
   server-address ip-address ;
   update-server;
   vendor-id vendor-id ;
}
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

dynamic-call-admission-control

Syntax

```
dynamic-call-admission-control {
   activation-priority priority;
   bearer-bandwidth-limit kilobits-per-second;
}
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number*]

Release Information

Statement introduced in Release 8.2 of Junos OS.

Description

This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure dynamic call admission control (CAC). Dynamic CAC provides enhanced control over WAN bandwidth. When dynamic CAC is configured on an interface responsible for providing call bandwidth, the TGM550 informs the Media Gateway Controller (MGC) of the bandwidth limit available for voice packets on the interface and requests that the MGC block new calls when the bandwidth is exhausted.

Dynamic CAC must be configured on each J Series Services Router interface responsible for providing call bandwidth.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

encapsulation

Syntax

encapsulation
(cisco-hdlc | frame-relay | multilink-frame-relay-uni-nni | ppp)

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number*]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Specify logical link layer encapsulation.

cisco-hdlc—For normal mode (when the device is using only one B-channel). Cisco-compatible High-Level Data Link Control is a group of protocols for transmitting data between network points.

frame-relay—Configure a Frame Relay encapsulation when the physical interface has multiple logical units, and the units are either point to point or multipoint.

multilink-frame-relay-uni-nni—Link services interfaces functioning as FRF.16 bundles can use Multilink Frame Relay UNI NNI encapsulation.

ppp—For normal mode (when the device is using only one ISDN B-channel per call). Point-to-Point Protocol is for communication between two computers using a serial interface.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

fabric-options

Syntax

```
fabric-options {
   member-interfaces member-interface-name ;
}
```

Hierarchy Level

[edit interfaces *interface-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure fabric interface properties.

Options

The remaining statement is explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

family bridge

Syntax

```
family bridge {
  interface-mode {
    access vlan-id vlan-id |
    trunk {
      vlan-id-list vlan-list |
      vlan-rewrite translate from-vlan-id internal-vlan-id
    }
  }
}
```

Hierarchy Level [edit interfaces *interface* unit *unit*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure a Layer 2 logical interface.

NOTE: If a physical interface has a bridge family logical interface, it cannot have any other family type in its logical interfaces.

Options **interface-mode**—Either **access** or **trunk**:

- An access mode interface accepts untagged packets, assigns the specified VLAN identifier to the packet, and forwards the packet within the bridge domain that is configured with the matching VLAN identifier.
- A trunk mode interface accepts any packet tagged with a VLAN identifier that matches a specified list of VLAN identifiers.

  vlan-rewrite translate—Rewrites the ***from-vlan-id*** VLAN identifier with the ***internal-vlan-id*** in packets arriving on a Layer 2 trunk port. The ***internal-vlan-id*** must be in the ***vlan-list*** for the trunk port.

NOTE: The *from-vlan-id* and *internal-vlan-id* must not be the same VLAN identifier configured with the **native-vlan-id** statement for the trunk port.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

family inet

Syntax

```
family inet {
   address ip-address;
   }
}
```

Hierarchy Level

[edit interfaces *interface* unit *unit*]

Release Information

Statement introduced in a prior release of Junos OS.

Description

Assign an IP address to a logical interface.

Options

ipaddress—Specifies the IP address for the interface.

NOTE: You use family inet to assign an IPv4 address. You use family inet6 to assign an IPv6 address. An interface can be configured with both an IPv4 and IPv6 address.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

family inet6

Syntax

```
family inet6 {
   address ip-address;
   }
}
```

Hierarchy Level [edit interfaces *interface* unit *unit*]

Release Information Statement supported in Junos 10.2 for SRX Series and J Series devices.

Description Assign an IP address to a logical interface.

Options *ipaddress*—Specifies the IP address for the interface.

NOTE: You use family **inet6** to assign an IPv6 address. You use family **inet** to assign an IPv4 address. An interface can be configured with both an IPv4 and IPv6 address.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

flag

Syntax flag

Hierarchy Level [edit interfaces interface-name traceoptions]

Release Information Command introduced in Release 10.1 of Junos OS.

Description Define tracing operations for individual interfaces. To specify more than one tracing operation, include multiple flag statements.

Options

- **all**—Enable all interface trace flags
- **event** —Trace interface events
- **ipc**—Trace interface IPC messages
- **media**—Trace interface media changes
- **critical**—Trace critical events
- **major**—Trace major events

NOTE: MTU is limited to 1518 on this interface.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

flow-control

Syntax (flow-control | no-flow-control);

Hierarchy Level [edit interfaces *interface-name* fastether-options],
[edit interfaces *interface-name* gigether-options],
[edit interfaces *interface-name* redundant-ether-options]

Release Information Statement modified in Release 9.0 of Junos OS.

Description For Fast Ethernet, Gigabit Ethernet, and redundant Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the device to the remote side of the connection. Enabling flow control is useful when the device is a Gigabit Ethernet switch. Flow control is not supported on the 4-port Fast Ethernet ePIM.

Default Flow control is the default behavior.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

fpc

Syntax fpc;

Hierarchy Level [edit interfaces pic-set pic-set-name]

Release Information Command introduced in Release 9.6 of Junos OS.

Description Sets the PIC bundle and the FPC slot.

Options ***apply-groups***—Inherit configuration data from these groups.

apply-groups-except—Do not inherit configuration data from these groups.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

gsm-options

Syntax

```
gsm-options {
  select-profile profile-name;
  profiles {
    profile-name {
      sip-user-id simple-ip-user-id;
      sip-password simple-ip-password;
      access-point-name apn;
      authentication-method (pap | chap | none);
    }
  }
}
```

Hierarchy Level [edit interfaces *interface-name* cellular-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the 3G wireless modem interface to establish a data call with a Global System for Mobile Communications (GSM) cellular network.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

interface (PIC Bundle)

Syntax interface *interface-name*;

Hierarchy Level [edit interfaces pic-set pic-set-name]

Release Information Command introduced in Release 9.6 of Junos OS.

Description Sets the PIC bundle and the interface.

Options ***apply-groups***— Groups from which to inherit configuration data.

apply-groups-except— Do not inherit configuration data from these groups.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

lacp

Syntax

```
lacp {
   (active | passive);
   periodic (fast | slow);
}
```

Hierarchy Level [edit interfaces *interface-name* redundant-ether-options]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description For redundant Ethernet interfaces in a chassis cluster only, configure Link Aggregation Control Protocol (LACP).

Options

- **active**—Initiate transmission of LACP packets.
- **passive**—Respond to LACP packets.

Default: If you do not specify **lacp** as either **active** or **passive**, LACP remains off (the default).

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

latency

Syntax latency <*value*>;

Hierarchy Level [edit interfaces *interface-name* radio—router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This option controls the latency weight (value 0–100).

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

lease-time

Syntax lease-time *seconds* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options *seconds* —Request time to negotiate and exchange information.

Range: 60 through 2,147,483,647 seconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

line-rate

Syntax line-rate

Hierarchy Level [edit interfaces *interfaces name* shdsl-options]

Release Information Command introduced in Release 10.0 of Junos OS.

Description Specify a line rate for an G.SHDSL interface.

Options
- **auto**— Automatically selects a line rate.
- **value** — Select the values between 192 kbps and 22784 kbps for the speed of transmission of data on the G.SHDSL connection.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

link-speed

Syntax **link-speed** ***speed*** **;**

Hierarchy Level **[edit interfaces** ***interface-name*** **redundant-ether-options]**

Release Information Statement modified in Release 9.0 of Junos OS.

Description For redundant Ethernet interfaces in a chassis cluster only, set the required link speed.

Options ***speed*** —For redundant Ethernet links, you can specify ***speed*** in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

loopback

Syntax **(loopback | no-loopback);**

Hierarchy Level **[edit interfaces** ***interface-name*** **redundant-ether-options]**

Release Information Statement modified in Release 9.0 of Junos OS.

Description For Fast Ethernet, Gigabit Ethernet, and redundant Ethernet interfaces, enable or disable loopback mode.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

media-type

Syntax media-type

Hierarchy Level [edit interfaces *interface-name* media-type]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Configure the operating modes for the 2-Port 10 Gigabit Ethernet XPIM.

Options
- copper
- fiber

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

member-interfaces

Syntax member-interfaces ***member-interface-name*** ;

Hierarchy Level [edit interfaces *interface-name* fabric-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the member interface name. Member interfaces that connect to each other must be of the same type.

Options ***member-interface-name*** —Member interface name.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

minimum-links

Syntax **minimum-links** *number* ;

Hierarchy Level **[edit interfaces** *interface-name* **redundant-ether-options]**

Release Information Statement added in Release 10.1 of Junos OS.

Description For redundant Ethernet interfaces configured as 802.3ad redundant Ethernet interface link aggregation groups (LAGs) in a chassis cluster only, set the required minimum number of physical child links on the primary node that must be working to prevent the interface from being down. Interfaces configured as redundant Ethernet interface LAGs typically have between 4 and 16 physical interfaces, but only half, those on the primary node, are relevant to the minimum-links setting.

If the number of operating interfaces on the primary node falls below the configured value, it will cause the interface to be down even if some of the interfaces are still working.

Options ***number***—For redundant Ethernet interface link aggregation group links, specify the number of physical child links on the primary node in the redundant Ethernet interface that must be working. The default **minimum-links** value is 1. The maximum value is half of the total number of physical child interfaces bound to the redundant Ethernet interface being configured or 8, whichever is smaller.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

native-vlan-id

Syntax native-vlan-id *vlan-id*;

Hierarchy Level [edit interfaces *interface*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure VLAN identifier for untagged packets received on the physical interface of a trunk mode interface.

Options ***vlan-id***—Configures a VLAN identifier for untagged packets. Enter a number from 0 through 4094.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

next-hop-tunnel

Syntax **next-hop-tunnel** *gateway-address* **ipsec-vpn** *vpn-name* **;**

Hierarchy Level **[edit interfaces** *interface-name* **unit** *logical-unit-number* **family** *family-name***]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description For the secure tunnel (**st**) interface, create entries in the Next-Hop Tunnel Binding (NHTB) table, which is used to map the next-hop gateway IP address to a particular IP Security (IPsec) Virtual Private Network (VPN) tunnel. NHTB allows the binding of multiple IPsec VPN tunnels to a single IPsec tunnel interface.

Options ***gateway-address*** —Next-hop gateway IP address.

ipsec-vpn ***vpn-name*** —VPN to which the next-hop gateway IP address is mapped.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

no-flow-control

See **flow-control**

no-loopback

See **loopback**

no-source-filtering

See **source-filtering**

Copyright © 2011, Juniper Networks, Inc.

periodic

Syntax **periodic (fast | slow);**

Hierarchy Level **[edit interfaces *interface-name* redundant-ether-options lacp]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description For redundant Ethernet interfaces in a chassis cluster only, configure the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs) by configuring the **periodic** statement on the interfaces on the local side. It is the configuration on the local side that specifies the behavior of the remote side. That is, the remote side transmits link aggregation control PDUs at the specified interval.

Options

- **fast**—Transmit link aggregation control PDUs every second.
- **slow**—Transmit link aggregation control PDUs every 30 seconds.

Default: **fast**

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

pic-mode

Syntax pic-mode

Hierarchy Level [set chassis fpc *fpc slot-number* pic *pic slot-number* shdsl]

Release Information Command introduced in Release 10.0 of Junos OS.

Description Specify the operating mode for the G.SHDSL interface.

Options

- 1-port-atm — 8-wire mode
- 2-port-atm —4-wire mode
- 4-port-atm —2-wire mode

NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the edit chassis fpc command becomes edit chassis node *node-id*fpc.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

profiles

Syntax

```
profiles {
  profile-name {
    sip-user-id simple-ip-user-id;
    sip-password simple-ip-password;
    access-point-name apn;
    authentication-method (pap | chap | none);
  }
}
```

Hierarchy Level [edit interfaces *interface-name* cellular-options gsm-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a profile to establish a data call with a Global System for Mobile Communications (GSM) cellular network. You can configure up to 16 profiles.

Options ***profile-name***—Name of the profile.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

promiscuous-mode

Syntax promiscuous-mode;

Hierarchy Level [edit interfaces *interface*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Enable promiscuous mode on Layer 3 Ethernet interfaces. When promiscuous mode is enabled on an interface, all packets received on the interface are sent to the central point or Services Processing Unit regardless of the destination MAC address of the packet.

You can also enable promiscuous mode on chassis cluster redundant Ethernet interfaces and on aggregated Ethernet interfaces. If you enable promiscuous mode on a redundant Ethernet interface, promiscuous mode is then enabled on any child physical interfaces. If you enable promiscuous mode on an aggregated Ethernet interface, promiscuous mode is then enabled on all member interfaces.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

quality

Syntax quality *<value>*;

Hierarchy Level [edit interfaces *interface-name* radio—router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This option controls relative link quality weight (value 0–100).

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

radio-router

Syntax

```
radio-router {
bandwidth;
   credit {
   interval;
   }
   latency;
   quality;
   resource;
threshold;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Point-to-Point Protocol over Ethernet (PPPoE)-based radio-to-router protocols include messages that define how an external system will provide the device with timely information about the quality of a link's connection. They also include a flow control mechanism to indicate how much data the device can forward. The device can then use the information provided in the PPPoE messages to dynamically adjust the interface speed of PPP links.

Options The remaining statements are explained separately.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

redundancy-group

Syntax **redundancy-group** *number* ;

Hierarchy Level **[edit interfaces** *interface-name* **redundant-ether-options]**

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the redundancy group that a redundant Ethernet interface belongs to.

Options ***number*** —Number of the redundancy group that the redundant interface belongs to. Failover properties of the interface are inherited from the redundancy group.

Range: 1 through 255

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

redundant-ether-options

Syntax

```
redundant-ether-options {
   (flow-control | no-flow-control);
   lacp {
      (active | passive);
      periodic (fast | slow);
   }
   link-speed speed;
   (loopback | no-loopback);
   minimum-links number;
   redundancy-group number;
   source-address-filter mac-address;
   (source-filtering | no-source-filtering);
}
```

Hierarchy Level **[edit interfaces** *interface-name***]**

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Configure Ethernet redundancy options for a chassis cluster.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

redundant-parent (Fast Ethernet Options)

Syntax **redundant-parent** ***interface-name*** **;**

Hierarchy Level **[edit interfaces** ***interface-name*** **fastether-options]**

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Configure Fast Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

Options ***interface*** —Parent redundant interface of the Fast Ethernet interface.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

redundant-parent (Gigabit Ethernet Options)

Syntax **redundant-parent** ***interface-name*** **;**

Hierarchy Level **[edit interfaces** ***interface-name*** **gigether-options]**

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Configure Gigabit Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

Options ***interface*** —Parent redundant interface of the Gigabit Ethernet interface.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

resource

Syntax resource <*value*>;

Hierarchy Level [edit interfaces *interface-name* radio—router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This option controls the resource weight (value 1–100).

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

retransmission-attempt

Syntax retransmission-attempt *number* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.

Options *number* —Number of attempts to retransmit the packet.
Range: 0 through 6
Default: 4

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

retransmission-interval

Syntax retransmission-interval ***seconds*** ;

Hierarchy Level [edit **interfaces** ***interface-name*** unit ***logical-unit-number*** family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time between successive retransmission attempts.

Options ***seconds*** —Number of seconds between successive retransmission.
Range: 4 through 64 seconds
Default: 4 seconds

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

roaming-mode

Syntax **roaming-mode (home-only | automatic)**

Hierarchy Level **[edit interfaces** *interface-name* **cellular-options]**

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Specify whether the 3G wireless modem interface can access networks other than the home network.

Options **home-only**—No roaming is allowed.

automatic—Allows access to networks other than the home network. This is the default.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

select-profile

Syntax **select-profile** *profile-name*

Hierarchy Level **[edit interfaces** *interface-name* **cellular-options gsm-options]**

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Select the active profile to establish a data call with a Global System for Mobile Communications (GSM) cellular network.

Options ***profile-name***—Name of a configured profile that is to be used to establish a data call.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

server-address

Syntax server-address ***ip-address*** ;

Hierarchy Level [edit **interfaces** ***interface-name*** unit ***logical-unit-number*** family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the preferred DHCP server address that is sent to DHCP clients.

Options ***ip-address*** —DHCP server address.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

simple-filter

Syntax

```
simple-filter{
   input filter-name;
}
```

Hierarchy Level [edit interfaces *interfaces-name* unit *logical-unit-number* family *family-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Apply a simple filter to an interface. You can apply simple filters on ingress interfaces only.

Options input ***filter-name***: Name of one filter to evaluate when packets are received on the interface.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

sip-password

Syntax sip-password *simple-ip-password*;

Hierarchy Level [edit interfaces *interface-name* cellular-options gsm-options profiles *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the password provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

Options ***simple-ip-password***—Password.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

sip-user-id

Syntax **sip-user-id** *simple-ip-user-id*;

Hierarchy Level **[edit interfaces** *interface-name* **cellular-options gsm-options profiles** *profile-name***]**

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the username provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

Options ***simple-ip-user-id***—Username.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

source-address-filter

Syntax **source-address-filter** ***mac-address*** ;

Hierarchy Level **[edit interfaces** ***interface-name*** **redundant-ether-options]**

Release Information Statement modified in Release 9.0 of Junos OS.

Description For redundant Ethernet interfaces, specify the MAC addresses from which the interface can receive packets. For this statement to have any effect, you must include the **source-filtering** statement in the configuration to enable source address filtering.

Be sure to update the MAC address if the remote Ethernet card is replaced. Replacing the interface card changes the MAC address. Otherwise, the interface cannot receive packets from the new card.

Options ***mac-address*** —MAC address filter. You can specify the MAC address as six hexadecimal bytes in one of the following formats: ***nn:nn:nn:nn:nn:nn:nn*** (for example, **00:11:22:33:44:55**) or ***nnnn:nnnn:nnnn*** (for example, **0011.2233.4455**). You can configure up to 64 source addresses. To specify more than one address, include multiple ***mac-address*** options in the **source-address-filter** statement.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

source-filtering

Syntax **(source-filtering | no-source-filtering);**

Hierarchy Level **[edit interfaces** ***interface-name*** **redundant-ether-options]**

Release Information Statement modified in Release 9.0 of Junos OS.

Description For redundant Ethernet interfaces, enable the filtering of MAC source addresses, which blocks all incoming packets to that interface. To allow the interface to receive packets from specific MAC addresses, include the **source-address-filter** statement.

If the remote Ethernet card is changed, the interface cannot receive packets from the new card because it has a different MAC address.

By default, source address filtering is disabled.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

speed

Syntax speed;

Hierarchy Level [edit interfaces *interface-name* speed]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Configure the operating speed for the 2-Port 10 Gigabit Ethernet XPIM.

Options
- 100m — Link speed of 100 Mbps
- 10g — Link speed of 10 Gbps
- 10m — Link speed of 10 Mbps
- 1g — Link speed of 1 Gbps

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

threshold

Syntax threshold <*value*>;

Hierarchy Level [edit interfaces *interface-name* radio–router]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description This option controls the percentage of bandwidth change required for routing updates.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

traceoptions

Syntax traceoptions

Hierarchy Level [edit interfaces interface-name traceoptions]

Release Information Command introduced in Release 10.1 of Junos OS.

Description Define tracing operations for individual interfaces. To specify more than one tracing operation, include multiple flag statements.

Options
- **flag** - Tracing parameters

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

update-server

Syntax update-server;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Propagate DHCP options to a local DHCP server.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

unframed | no-unframed

Syntax (unframed | no-unframed);

Hierarchy Level [edit interfaces *interface-name* t3-options]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Enables or disables framing for the T3 interface on a 1-Port Clear Channel DS3/E3 GPIM on an SRX650 device. By default, unframed mode is enabled. Select no-unframed to enable framing. Select unframed to return to the default mode.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

vbr rate

Syntax vbr rate;

Hierarchy Level [edit interfaces interface-name atm-options vpi vpi-identifier shaping]

Release Information Command introduced in Release 9.5 of Junos OS.

Description For ATM encapsulation only, define a variable bit rate bandwidth utilization in the traffic-shaping profile.

Options Burst Size - The maximum burst size that can be sent at the peak rate.

Peak Rate - The maximum instantaneous rate at which the user will transmit.

Sustained Rate - The average rate as measured over a long interval.

CDVT - Cell Delay Variation Tolerance in microseconds (range: 1 – 9999).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

vdsl-profile

Syntax vdsl-profile

Hierarchy Level [edit interfaces interface-name vdsl-options]

Release Information Command introduced in Release 10.1 of Junos OS.

Description Configure the type of VDSL2 profiles. A profile is a table that contains a list of preconfigured VDSL2 settings.

Options

- Auto (default)
- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

vendor-id

Syntax vendor-id ***vendor-id*** ;

Hierarchy Level [edit interfaces ***interface-name*** unit ***logical-unit-number*** family *family-name* dhcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

Options ***vendor-id*** —vendor class ID.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

vlan-tagging

Syntax vlan-tagging native-vlan-id *vlan-id*;

Hierarchy Level [edit interfaces *interface*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure VLAN identifier for untagged packets received on the physical interface of a trunk mode interface.

Options **native-vlan-id**—Configures a VLAN identifier for untagged packets. Enter a number from 0 through 4094.

Required Privilege Level **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

web-authentication

Syntax
```
web-authentication {
  http;
}
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* address *address*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the Web authentication process for firewall user authentication.

http—Enable HTTP service.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 12

Power Over Ethernet Hierarchy and Statements

This section contains the following topics:

- PoE Configuration Statement Hierarchy on page 195

PoE Configuration Statement Hierarchy

To configure Power over Ethernet options, use the configuration statements in the **poe** configuration hierarchy. Statement descriptions that are exclusive to the J Series and SRX Series devices running Junos OS are described in this chapter.

```
poe {
  management type;
    guard-band watts;
    interface (all | interface-name) {
    disable ;
      maximum-power watts ;
      priority value;
      telemetries {
      disable;
        duration hours;
      interval minutes;
    }
  }
}
```

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

disable

Syntax disable

Hierarchy Level [edit poe interface (all | interface-name)],
[edit poe interface (all | interface-name) telemetries]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Disables the PoE capabilities of the port. If PoE capabilities are disabled for a port, the port operates as a standard network access port. If the disable statement is specified after the telemetries statement, logging of PoE power consumption for the port is disabled. To disable monitoring and retain the stored interval and duration values for possible future use, you can specify the disable sub statement in the sub stanza for telemetries. Similarly for retaining the port configuration but disabling the PoE feature on the port, disable can be used in sub stanza for interface.

Default The PoE capabilities are automatically enabled when a PoE interface is set. Specifying the telemetries statement enables monitoring of PoE per-port power consumption.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

duration

Syntax duration hours;

Hierarchy Level [edit poe interface (all | interface-name) telemetries]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Modifies the duration for which telemetry records are stored. If telemetry logging continues beyond the specified duration, the older records are discarded one by one as new records are collected.

Options hours— Hours for which telemetry data should be retained.

Range — 1 through 24 hours

Default— 1 hour

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

guard-band

Syntax guard-band watts;

Hierarchy Level [edit poe]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Reserves the specified amount of power for the SRX Series device in case of a spike in PoE consumption.

Options watts—Amount of power to be reserved for the SRX Series device in case of a spike in PoE consumption.

Range — 0 through 19 W

Default— 0 W

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

interface

Syntax

```
interface (all | interface-name) {
  disable;
    maximum-power watts;
    priority value;
    telemetries {
    disable;
      interval minutes;
    duration hours;
  }
}
```

Hierarchy Level [edit poe]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enable a PoE interface for a PoE port. The PoE interface must be enabled in order for the port to provide power to a connected powered device.

Default The PoE interface is enabled by default

Options

all— Apply the configuration to all interfaces on the SRX Series device that have not been explicitly configured otherwise.

interface-name— Explicitly configure a specific interface.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
The remaining statements are explained separately.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

interval

Syntax interval minutes;

Hierarchy Level [edit poe interface (all | interface-name) telemetries]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Modifies the interval for logging telemetries if you are monitoring the per-port power consumption for PoE interfaces.

Options minutes—Interval at which data is logged.

Range —1 through 30 minutes

Default — 5 minutes

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

management

Syntax management type;

Hierarchy Level [edit poe]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Designates how the SRX Series device allocates power to the PoE ports.

Default static

Options type—Management type:

static—When a powered device is connected to a PoE port, the power allocated to it is equal to the maximum power configured for the port.

class—When a powered device is connected to a PoE port, the power allocated to it is equal to the maximum power for the class as defined by the IEEE 802.3 AF standard.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Interfaces Configuration Guide for Security Devices*

maximum-power

Syntax maximum-power watts;

Hierarchy Level [edit poe interface (all | interface-name)]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Maximum amount of power that can be supplied to the port

Default 15.4 W

Options Watts

Range —0 through 15.4

Default—15.4 W

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

priority

Syntax priority value;

Hierarchy Level [edit poe interface (all | interface-name)]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Sets the priority of individual ports. When it is not possible to maintain power to all connected ports, lower-priority ports are powered off before higher priority ports. When a new device is connected on a higher-priority port, a lower-priority port will be powered off automatically if available power is insufficient to power on the higher-priority port. Note that for ports with the same priority configuration, ports on the left are given higher priority than the ports on the right.

Default low

Options value—high or low:

high—Specify that this port is to be treated as high priority in terms of power allocation

low—Specify that this port is to be treated as low priority in terms of power allocation.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Interfaces Configuration Guide for Security Devices*

telemetries

Syntax

```
telemetries {
   disable;
      duration hours;
   interval minutes;
}
```

Hierarchy Level

[edit poe interface (all | interface-name)]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Allows logging of per-port PoE power consumption. The telemetries section must be explicitly specified to enable logging. If left unspecified, telemetries is disabled by default.

Default

If the telemetries statement is specified, logging is enabled with the default values for interval and duration.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Power Over Ethernet Hierarchy and Statements on page 195
- *Junos OS Interfaces Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 13

Policy-Options Hierarchy and Statements

This section contains the following topics:

- Policy-Options Configuration Statement Hierarchy on page 203

Policy-Options Configuration Statement Hierarchy

Use the statements in the **policy-options** configuration hierarchy to configure routing policies that control information from routing protocols that the device imports into its routing table and exports to its neighbors.

```
policy-options {
  as-path name regular-expression ;
  as-path-group group-name;
  community name {
    invert-match;
    members [ community-ids];
  }
  condition condition-name {
    if-route-exists address table table-name;
    route-active-on (node0 | node1);
  }
  damping name{
    disable;
    half-life minutes;
    max-suppress minutes;
    reuse number;
    suppress number;
  }
  policy-statement policy-name {
    term term-name {
      default-action (accept | reject);
      from {
        family family-name;
        match-conditions;
        policy subroutine- policy-name;
        prefix-list name;
        route-filter destination-prefix match-type < actions>;
        source-address-filter destination-prefix match-type <actions>;
      }
      to {
        match-conditions;
```

```
            policy subroutine- policy-name;
          }
          then actions;
        }
      }
      prefix-list name {
        ip-addresses;
      }
    }
```

Related Documentation

- *Junos OS Policy Framework Configuration Guide*
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

condition

Syntax

```
condition condition-name {
  if-route-exists address table table-name ;
  route-active-on (node0 | node1);
}
```

Hierarchy Level

[edit policy-options]

Release Information

Statement introduced in Release 9.0 of Junos OS.

Description

For chassis cluster configurations, specify the match condition for use in routing to a redundant Ethernet (**reth**) interface.

Options

condition-name —Name of the routing policy match condition.

The remaining statement is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

route-active-on

Syntax route-active-on (node0 | node1);

Hierarchy Level [edit policy-options condition *condition-name*]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description For chassis cluster configurations, identify the device (node) on which a route is active.

Options **node0** | **node1**—Node in a chassis cluster.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 14

Protocols Hierarchy and Statements

This section contains the following topics:

- Protocols Configuration Statement Hierarchy on page 207

Protocols Configuration Statement Hierarchy

Use the **protocols** configuration hierarchy statements to configure routing protocols, including End System-to-Intermediate System (ES-IS), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Routing Information Protocol Next Generation (RIPng), Border Gateway Protocol (BGP), and Layer 2 address learning and forwarding.

```
protocols {
  bfd {
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  bgp {
    accept-remote-nexthop;
    advertise-inactive;
    advertise-peer-as;
    authentication-algorithm algorithm ;
    authentication-key key ;
    authentication-key-chain key-chain ;
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      holddown-interval milliseconds;
      local-address ip-address ;
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      minimum-receive-ttl milliseconds ;
      multiplier number ;
      neighbor address ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
```

```
    }
    version (0 | 1);
  }
  cluster cluster-identifier;
  damping;
  description text-description ;
  disable;
  export [ policy-name ];
  family {
    (inet | inet-mvpn | inet-vpn | inet6 | inet6-mvpn | inet6-vpn | iso-vpn | l2-vpn) {
      (any | flow | multicast | unicast | signaling) {
        prefix-limit {
          maximum number ;
          teardown < percentage > <idle-timeout (forever | minutes )>;
        }
        rib-group group-name ;
      }
      labeled-unicast {
        aggregate-label {
          community community-name :
        }
        explicit-null {
          connected-only;
        }
        per-group-label;
        prefix-limit {
          maximum number ;
          teardown < percentage > <idle-timeout (forever | minutes )>;
        }
        resolve-vpn;
        rib inet.3;
        rib-group group-name ;
        traffic-statistics {
          file filename <files number > <match regular-expression >
          <size maximum-file-size > <world-readable | no-world-readable>;
          interval seconds ;
        }
      }
    }
    route-target {
      advertise-default;
      external-paths number ;
      prefix-limit {
        maximum number ;
        teardown < percentage > <idle-timeout (forever | minutes )>;
      }
    }
  }
  graceful-restart {
    disable;
    restart-time seconds ;
    stale-routes-time seconds ;
  }
  group group-name {
    bgp-options ;
    peer-as autonomous-system ;
```


Copyright © 2011, Juniper Networks, Inc.

```
        type type ;
        neighbor address ;
      }
      hold-time seconds ;
      import [ policy-name ];
      include-mp-next-hop;
      keep (all | none);
      local-address address ;
      local-as autonomous-system <private> <loops loops >;
      local-preference local-preference ;
      log-updown;
      metric-out ( metric | minimum-igp < offset > | igp < offset >);
      multihop < ttl-value >;
      no-advertise-peer-as;
      no-aggregator-id;
      no-client-reflect;
      out-delay seconds ;
      passive;
      path-selection {
        (always-compare-med | cisco-non-deterministic | external-router-id);
        med-plus-igp {
          igp-multiplier number ;
          med-multiplier number ;
        }
      }
      peer-as autonomous-system ;
      preference preference ;
      remove-private;
      tcp-mss segment-size ;
      traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
      vpn-apply-export;
    }
    connections {
      interface-switch interface-switch-name {
        interface interface-name ;
      }
      lsp-switch lsp-switch-name {
        receive-lsp path-name ;
        transmit-lsp path-name ;
      }
      remote-interface-switch {
        interface interface-name ;
        receive-lsp path-name ;
        transmit-lsp path-name ;
      }
    }
    dot1x {
      authenticator {
        authentication-profile-name profile-name ;
        interface interface-name {
          guest-vlan vlan-name;
          mac-radius;
```

```
            maximum-requests request-number ;
            quiet-period seconds ;
            (reauthentication seconds | no-reauthentication);
            retries number ;
            server-fail deny | permit | use-cache | vlan vlan-name | vlan vlan-id;
            server-timeout seconds ;
            supplicant (multiple | single | single-secure);
            supplicant-timeout seconds ;
            transmit-period seconds ;
          }
          server-reject-vlan vlan-name | vlan-id;
          static mac-address {
            interface interface-name;
            vlan-assignment ( vlan-id | vlan-name);
          }
        }
        traceoptions {
          file filename <files number >
          <size maximum-file-size > <world-readable | no-world-readable>;
          flag flag <disable>;
        }
      }
      dvmrp {
        disable;
        export [ policy-name ];
        import [ policy-name ];
        interface interface-name {
          disable;
          hold-time seconds ;
          metric value ;
          mode (forwarding | unicast-routing);
        }
        rib-group group-name ;
        traceoptions {
          file filename <files number >
          <size maximum-file-size > <world-readable | no-world-readable>;
          flag flag < flag-modifier > <disable>;
        }
      }
      esis {
        disable;
        graceful-restart {
          disable;
          restart-duration seconds;
        }
        interface (interface-name | all) {
          disable;
          end-system-configuration-timer seconds;
          hold-time seconds;
        }
        preference preference;
        traceoptions {
          file filename <files number> <size maximum-file-size>
          <world-readable | no-world-readable>;
          flag flag <flag-modifier> <disable>;
        }
```


Copyright © 2011, Juniper Networks, Inc.

```
}
gvrp {
  disable;
  interface interface-name {
    disable;
  }
  join-timer milliseconds ;
  leave-timer milliseconds ;
  leaveall-timer milliseconds ;
}
igmp {
  accounting;
  interface interface-name {
    (accounting | no-accounting);
    disable;
    immediate-leave;
    promiscuous-mode;
    ssm-map ssm-map ;
    static {
      group group-address {
        source source-address ;
      }
    }
    version number ;
  }
  query-interval seconds ;
  query-last-member-interval seconds ;
  query-response-interval seconds ;
  robust-count robust-count ;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
igmp-snooping {
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable> <match regex>;
    flag flag ;
  }
  vlan ( vlan-id | vlan-number {
    disable;
    immediate-leave;
    interface interface-name {
      multicast-router-interface;
      static {
        group ip-address ;
      }
    }
    query-interval seconds ;
    query-last-member-interval seconds ;
    query-response-interval seconds ;
    robust-count number ;
  }
}
```

```
isis {
  clns-routing;
  disable;
  export [ policy-names ];
  graceful-restart {
    disable;
    helper-disable;
    restart-duration seconds ;
  }
  ignore-attached-bit;
  interface (all | interface-name ) {
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
      }
      multiplier number ;
      version (1 | automatic);
    }
    checksum;
    csnp-interval ( seconds | disable);
    disable;
    hello-padding (adaptive | loose | strict);
    ldp-synchronization {
      disable;
      hold-time seconds ;
    }
    level level-number {
      disable;
      hello-authentication-key key;
      hello-authentication-type authentication ;
      hello-interval seconds ;
      hold-time seconds ;
      ipv4-multicast-metric number ;
      ipv6-multicast-metric number ;
      ipv6-unicast-metric number ;
      metric metric ;
      passive;
      priority number ;
      te-metric metric ;
    }
    lsp-interval milliseconds ;
    mesh-group ( value | blocked);
    no-adjacency-down-notification;
    no-ipv4-multicast;
    no-ipv6-multicast;
    no-ipv6-unicast;
    no-unicast-topology;
    passive;
    point-to-point;
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
    label-switched-path name level level metric metric ;
    level level-number {
      authentication-key key ;
      authentication-type authentication ;
      disable;
      external-preference preference ;
      no-csnp-authentication;
      no-hello-authentication;
      no-psnp-authentication;
      preference preference ;
      prefix-export-limit number ;
      wide-metrics-only;
    }
    loose-authentication-check;
    lsp-lifetime seconds ;
    no-adjacency-holddown;
    no-authentication-check;
    no-ipv4-routing;
    no-ipv6-routing;
    overload {
      advertise-high-metrics;
      timeout seconds ;
    }
    reference-bandwidth reference-bandwidth ;
    rib-group {
      inet group--name ;
      inet6 group--name ;
    }
    spf-options {
      delay milliseconds ;
      holddown milliseconds ;
      rapid-runs number ;
    }
    topologies {
      ipv4-multicast;
      ipv6-unicast;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
    traffic-engineering {
      disable;
      ipv4-multicast-rpf-routes;
      shortcuts <ignore-lsp-metrics>;
    }
  }
  l2-learning {
    global-mac-limit limit {
    packet-action-drop
    }
    global-mac-table-aging-time seconds;
    global-no-mac-learning;
  }
  l2circuit {
```

```
    local-switching {
      interface interface-name {
        description text-description ;
        end-interface {
          interface interface-name ;
          protect-interface interface-name ;
        }
        ignore-mtu-mismatch;
        protect-interface interface-name ;
      }
    }
    neighbor address {
      interface interface-name {
        bandwidth (ct0 class0 | ct1 class1 | ct2 class2 | ct3 class3 );
        community community ;
        (control-word | no-control-word);
        description text-description ;
        ignore-encapsulation-mismatch;
        mtu mtu ;
        protect-interface interface-name ;
        psn-tunnel-endpoint psn-tunnel-endpoint ;
        virtual-circuit-id circuit-id ;
      }
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  lacp {
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
    layer2-control {
      mac-rewrite {
        interface interface-name {
          protocol protocol-name ;
        }
      }
      nonstop-bridging {
        mac-rewrite {
          interface interface-name {
            protocol protocol-name ;
          }
        }
        traceoptions {
          file filename <files number >
          <size maximum-file-size > <world-readable | no-world-readable>;
          flag flag ;
        }
      }
      traceoptions {
        file filename <files number >
```

 Copyright © 2011, Juniper Networks, Inc.

```
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
      }
    }
    ldp {
      (deaggregate | no-deaggregate);
      egress-policy [ policy-name ];
      explicit-null;
      export [ policy-name ];
      graceful-restart {
        disable;
        helper-disable;
        maximum-recovery-time seconds ;
        recovery-time seconds ;
      }
      import [ policy-name ];
      interface interface-name {
        disable;
        hello-interval seconds ;
        hold-time seconds ;
        transport-address (interface | router-id);
      }
      keepalive-interval seconds ;
      keepalive-timeout seconds ;
      l2-smart-policy;
      log-updown {
        trap {
          disable;
        }
      }
      next-hop {
        merged {
          policy [ policy-name ];
        }
      }
      no-forwarding;
      oam {
        bfd-liveness-detection {
          detection-time {
            threshold milliseconds ;
          }
          minimum-interval milliseconds ;
          minimum-receive-interval milliseconds ;
          multiplier number ;
          transmit-interval {
            minimum-interval milliseconds ;
            threshold milliseconds ;
          }
          version (0 | 1 | automatic);
        }
        fec class-address {
          (bfd-liveness-detection | no-bfd-liveness-detection);
          periodic-traceroute flags ;
        }
      }
      policing {
```

```
        fec class-address {
          ingress-traffic filter-name ;
          transit-traffic filter-name ;
        }
      }
      preference preference ;
      session session-address {
        authentication-algorithm algorithm ;
        authentication-key key ;
        authentication-key-chain key-chain ;
      }
      strict-targeted-hellos;
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
      track-igp-metric;
      traffic-statistics {
        file filename <files number > < match regular-expression >
        <size maximum-file-size > <world-readable | no-world-readable>;
        interval seconds ;
        no-penultimate-hop;
      }
      transport-address (interface | router-id);
    }
    link-management {
      peer peer-name {
        address address ;
        control-channel [ control-channel-interfaces ];
        lmp-control-channel interface-name {
          remote-address address ;
        }
        lmp-protocol {
          hello-dead-interval milliseconds ;
          hello-interval milliseconds ;
          passive;
          retransmission-interval milliseconds ;
          retry-limit number ;
        }
        te-link [ te-link-names ];
      }
      te-link te-link-name {
        disable;
        interface interface-name {
          disable;
          local-address address ;
          remote-address address ;
          remote-id id-number ;
        }
        local-address address ;
        remote-address address ;
        remote-id id-number ;
        te-metric te-metric ;
      }
      traceoptions {
```

 Copyright © 2011, Juniper Networks, Inc.

```
        file filename <files number> <size maximum-file-size>
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    mld {
      interface interface-name {
        disable;
        immediate-leave;
        ssm-map ssm-map ;
        static {
          group group-address {
            source source-address ;
          }
        }
        version number ;
      }
      query-interval seconds ;
      query-last-member-interval seconds ;
      query-response-interval seconds ;
      robust-count robust-count ;
      traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    mpls {
      disable;
      admin-down;
      admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
      }
      admin-groups {
        group-name group-value ;
      }
      advertise-hold-time seconds ;
      auto-policing {
        class all policer-action;
        class ctnumber (drop | loss-priority-high | loss-priority-low);
      }
      bandwidth bps ;
      class-of-service cos-value ;
      diffserv-te {
        bandwidth-model {
          extended-mam;
          mam;
          rdm;
        }
        te-class-matrix {
          tenumber {
            priority priority ;
            traffic-class {
              ctnumber priority priority ;
```

```
        }
      }
    }
  }
  expand-loose-hop;
  explicit-null;
  hop-limit number ;
  icmp-tunneling;
  interface ( interface-name | all) {
    disable;
    admin-group {
      group-name ;
    }
    label-map ( in-label | default-route) {
      class-of-service value ;
      (discard | next-hop ( address | hostname | interface-name ) | reject);
      (pop | swap out-label );
      preference preference ;
      swap-push swap-label push-label ;
    }
  }
  ipv6-tunneling;
  label-switched-path lsp-name {
    disable;
    adaptive;
    admin-down;
    admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
    }
    associate-backup-pe-groups;
    auto-bandwidth {
      adjust-interval seconds ;
      adjust-threshold percent ;
      adjust-threshold-overflow-limit number ;
      maximum-bandwidth bps ;
      minimum-bandwidth bps ;
      monitor-bandwidth;
    }
    bandwidth bps ;
    class-of-service cos-value ;
    description;
    fast-reroute {
      bandwidth bps ;
      bandwidth-percent percent ;
      (exclude group-names | no-exclude);
      hop-limit number ;
      (include-all group-names | no-include-all);
      (include-any group-names | no-include-any);
    }
    from address ;
    hop-limit number ;
    install {
      destination-prefix / prefix-length <active>;
    }
```

 Copyright © 2011, Juniper Networks, Inc.

```
ldp-tunneling;
link-protection;
metric number ;
no-cspf;
no-decrement-ttl;
no-install-to-address;
node-link-protection;
oam {
  bfd-liveness-detection {
    detection-time threshold milliseconds ;
    failure-action teardown;
    minimum-interval milliseconds ;
    minimum-receive-interval milliseconds ;
    multiplier detection-time-multiplier ;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds ;
      threshold milliseconds ;
    }
    version bfd-version ;
  }
  traceoptions {
    file filename <files number > <match regular-expression >
    <size maximum-file-size > <world-readable | no-world-readable>;
    flag flag ;
  }
}
optimize-timer seconds ;
p2mp {
  path-name ;
}
policing {
  filter filter-name ;
  no-auto-policing;
}
preference preference ;
primary path-name {
  adaptive;
  admin-down;
  admin-group {
    exclude [ group-names ];
    include-all [ group-names ];
    include-any [ group-names ];
  }
  bandwidth bps ;
  class-of-service cos-value ;
  hop-limit number ;
  no-cspf;
  no-decrement-ttl;
  oam {
    bfd-liveness-detection {
      detection-time threshold milliseconds ;
      failure-action teardown;
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      multiplier detection-time-multiplier ;
```

```
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds ;
                threshold milliseconds ;
            }
            version bfd-version ;
        }
        traceoptions {
            file filename <files number > <match regular-expression >
            <size maximum-file-size > <world-readable | no-world-readable>;
            flag flag ;
        }
    }
    optimize-timer seconds ;
    preference preference ;
    priority setup-priority hold-priority ;
    (record | no-record);
    select {
        manual;
        unconditional;
    }
    standby;
}
priority setup-priority hold-priority ;
(random | least-fill | most-fill);
(record | no-record);
retry-limit number ;
retry-timer seconds ;
revert-timer seconds ;
secondary path-name {
    adaptive;
    admin-down;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps ;
    class-of-service cos-value ;
    hop-limit number ;
    no-cspf;
    no-decrement-ttl;
    oam {
        bfd-liveness-detection {
            detection-time threshold milliseconds ;
            failure-action teardown;
            minimum-interval milliseconds ;
            minimum-receive-interval milliseconds ;
            multiplier detection-time-multiplier ;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds ;
                threshold milliseconds ;
            }
            version bfd-version ;
        }
```

 Copyright © 2011, Juniper Networks, Inc.

```
            traceoptions {
                file filename <files number > <match regular-expression >
                <size maximum-file-size > <world-readable | no-world-readable>;
                flag flag ;
            }
        }
        optimize-timer seconds ;
        preference preference ;
        priority setup-priority hold-priority ;
        (record | no-record);
        select {
            manual;
            unconditional;
        }
        standby;
    }
    soft-preemption;
    standby;
    template;
    to address ;
    traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
    }
}
log-updown {
    (syslog | no-syslog);
    (trap | no-trap (mpls-lsp-traps | rfc3812-traps) );
    trap-path-down;
    trap-path-up;
}
no-cspf;
no-decrement-ttl;
no-propagate-ttl;
oam {
    bfd-liveness-detection {
        detection-time threshold milliseconds ;
        failure-action teardown;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        multiplier detection-time-multiplier ;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds ;
            threshold milliseconds ;
        }
        version bfd-version ;
    }
    traceoptions {
        file filename <files number > <match regular-expression >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
    }
}
optimize-aggressive;
```

```
    optimize-timer;
    path path-name {
      address <loose | strict>;
    }
    path-mtu {
      allow-fragmentation;
      rsvp {
        mtu-signaling;
      }
    }
    preference preference ;
    priority setup-priority hold-priority ;
    (record | no-record);
    revert-timer seconds ;
    rsvp-error-hold-time seconds ;
    smart-optimize-timer seconds ;
    standby;
    static-path inet {
      prefix {
        class-of-service value ;
        double-push bottom-value top-value ;
        next-hop ( address | interface-name );
        preference preference ;
        push out-label ;
        triple-push bottom-value middle-value top-value ;
      }
    }
    statistics {
      auto-bandwidth;
      file filename <files number> <size maximum-file-size >
      <world-readable | no-world-readable>;
      interval seconds ;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
    traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);
  }
  msdp {
    msdp-options ;
  }
  mstp {
    bpdu-block-on-edge;
    bridge-priority priority ;
    configuration-name name ;
    disable;
    forward-delay seconds ;
    hello-time seconds ;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost interface-cost ;
```


Copyright © 2011, Juniper Networks, Inc.

```
        disable;
        edge;
        mode (point-to-point | shared);
        no-root-port;
        priority interface-priority ;
      }
      max-age seconds ;
      max-hops number ;
      msti msti-id {
        bridge-priority priority ;
        interface interface-name {
          cost interface-cost ;
          disable;
          priority interface-priority ;
        }
        vlan [vlan-id];
      }
      revision-level number ;
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    oam {
      ethernet {
        connectivity-fault-management {
          action-profile profile-name {
            default-actions {
              interface-down;
            }
          }
          linktrace {
            age (10s | 30s | 1m | 10m | 30m);
            path-database-size number ;
          }
          maintenance-domain domain-name {
            level number;
            name-format (character-string | dns | mac+2oct | none);
            maintenance-association association-name {
              continuity-check {
                hold-interval minutes ;
                interval (10m | 10s | 1m | 1s | 100ms);
                loss-threshold number ;
              }
              mep mep-id {
                auto-discovery;
                direction (up | down);
                interface interface-name ;
                priority number ;
                remote-mep mep-id {
                  action-profile profile-name ;
                }
              }
              short-name-format (2octet | character-string | rfc-2685-vpn-id | vlan);
            }
```

```
            }
            traceoptions {
              file filename <files number > <match regular-expression >
              <size maximum-file-size > <world-readable | no-world-readable>;
              flag flag ;
            }
          }
          link-fault-management {
            action-profile profile-name {
              action {
                link-down;
                send-critical-event;
                syslog;
              }
              event {
                link-adjacency-loss;
                link-event-rate {
                  frame-error count ;
                  frame-period count ;
                  frame-period-summary count ;
                  symbol-period count ;
                }
                protocol-down;
              }
            }
            interface interface-name {
              apply-action-profile profile-name ;
              event-thresholds {
                frame-error count ;
                frame-period count ;
                frame-period-summary count ;
                symbol-period count ;
              }
              link-discovery (active | passive);
              negotiation-options {
                allow-remote-loopback;
                no-allow-link-events;
              }
              pdu-interval interval ;
              pdu-threshold threshold-value ;
            }
            traceoptions {
              file filename <files number > <match regular-expression >
              <size maximum-file-size > <world-readable | no-world-readable>;
              flag flag ;
            }
          }
        }
      }
      ospf {
        ospf-options ;
      }
      ospf3 {
        area area-id {
          area-range network/mask-length <restrict> <exact> <override-metric metric >;
          interface interface-name {
```


Copyright © 2011, Juniper Networks, Inc.

```
            disable;
            dead-interval seconds ;
            hello-interval seconds ;
            metric metric ;
            neighbor address <eligible>;
            passive;
            priority number ;
            retransmit-interval seconds ;
            transit-delay seconds ;
          }
          nssa {
            area-range network/mask-length <restrict> <exact>
            <override-metric metric >;
            default-lsa {
              default-metric metric ;
              metric-type type ;
              type-7;
            }
            (no-summaries | summaries);
          }
          stub <default-metric metric > <(no-summaries | summaries)>;
        }
        disable;
        export [ policy-names ];
        external-preference preference ;
        import [ policy-names ];
        overload {
          <timeout seconds >;
        }
        preference preference ;
        prefix-export-limit number ;
        reference-bandwidth reference-bandwidth ;
        rib-group group-name ;
        spf-options {
          delay milliseconds ;
          holddown milliseconds ;
          rapid-runs number ;
        }
        traceoptions {
          file filename <files number > <size maximum-file-size >
          <world-readable | no-world-readable>;
          flag flag < flag-modifier > <disable>;
        }
      }
      pgm {
        pgm-options ;
      }
      pim {
        pim-options ;
      }
      ppp {
        ppp-options ;
      }
      rip {
        authentication-key password ;
        authentication-type type ;
```

```
(check-zero | no-check-zero);
graceful-restart {
  disable;
  restart-time seconds ;
}
group group-name {
  bfd-liveness-detection {
    detection-time {
      threshold milliseconds ;
    }
    minimum-interval milliseconds ;
    minimum-receive-interval milliseconds ;
    transmit-interval {
      minimum-interval milliseconds ;
      threshold milliseconds ;
    }
    multiplier number ;
    version (0 | 1 | automatic);
  }
  export [ policy-names ];
  metric-out metric ;
  preference preference ;
  route-timeout seconds ;
  update-interval seconds ;
  neighbor neighbor-name {
    authentication-key password ;
    authentication-type type ;
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
      }
      multiplier number ;
      version (0 | 1 | automatic);
    }
    (check-zero | no-check-zero);
    import [ policy-names ];
    message-size number ;
    metric-in metric ;
    receive receive-options ;
    route-timeout seconds ;
    send send-options ;
    update-interval seconds ;
  }
}
holddown seconds ;
import [ policy-names ];
message-size number ;
metric-in metric ;
receive receive-options ;
rib-group group-name ;
```


Copyright © 2011, Juniper Networks, Inc.

```
  route-timeout seconds ;
  send send-options ;
  update-interval seconds ;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
ripng {
  ripng-options ;
}
router-advertisement {
  router-advertisement-configuration ;
}
router-discovery {
  address address {
    (advertise | ignore);
    (broadcast | multicast);
    (priority number | ineligible);
  }
  disable;
  interface interface-name {
    lifetime seconds ;
    max-advertisement-interval seconds ;
    min-advertisement-interval seconds ;
  }
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
rstp {
  bpdu-block-on-edge;
  bridge-priority priority ;
  disable;
  forward-delay seconds ;
  hello-time seconds ;
  interface interface-name {
    bpdu-timeout-action {
      alarm;
      block;
    }
    cost interface-cost ;
    disable;
    edge;
    mode (point-to-point | shared);
    no-root-port;
    priority interface-priority ;
  }
  max-age seconds ;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
```

```
    }
  }
  rsvp {
    rsvp-options ;
  }
  sap {
    sap-options ;
  }
  stp {
    bpdu-block-on-edge;
    bridge-priority priority ;
    disable;
    forward-delay seconds ;
    hello-time seconds ;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost interface-cost ;
      disable;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority ;
    }
    max-age seconds ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  vrrp {
    vrrp-options ;
  }
  vstp {
    disable;
    force-version stp;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost ;
      edge;
      mode (p2p | shared);
      no-root-port;
      priority interface-priority ;
    }
    vlan vlan-id {
      bridge-priority priority ;
      forward-delay seconds ;
      hello-time seconds ;
      interface interface-name {
        bpdu-timeout-action {
```


Copyright © 2011, Juniper Networks, Inc.

```
                alarm;
                block;
              }
              cost cost ;
              edge;
              mode (p2p | shared);
              no-root-port;
              priority interface-priority ;
            }
            max-age seconds ;
            traceoptions {
              file filename <files number >
              <size maximum-file-size > <world-readable | no-world-readable>;
              flag flag < flag-modifier > <disable>;
            }
          }
        }
      }
    }
```

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Routing Protocols Configuration Guide*
- *Junos OS Services Interfaces Configuration Guide*

disable

Syntax

disable;

Hierarchy Level

[edit protocols esis],
[edit protocols esis interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols esis],
[edit routing-instances *routing-instance-name* protocols esis interface *interface-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Disable ES-IS globally or on an interface.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

end-system-configuration-timer

Syntax end-system-configuration-timer *seconds*;

Hierarchy Level [edit protocols esis interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols esis interface *interface-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the ES-IS end system configuration timer.

Options ***seconds***—How often a system reports its availability to other systems.
Default: 180 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

esis

Syntax esis { ... }

Hierarchy Level [edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable ES-IS.

Options The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

graceful-restart

Syntax

```
graceful-restart {
   disable;
   restart-duration seconds;
}
```

Hierarchy Level [edit protocols esis]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure graceful restart for ES-IS.

Options **disable**—Disable graceful restart.

restart-duration *seconds*—Configure duration of the restart period.

Range: 30 through 300 seconds

Default: 180 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

hold-time

Syntax hold-time *seconds*;

Hierarchy Level [edit protocols esis interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols esis interface *interface-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Set the length of time a neighbor considers this interface to be operative (up) after receiving a hello packet. If the neighbor does not receive another hello packet within the specified time, it marks this interface as inoperative (down). The hold time itself is advertised in the hello packets.

Options ***seconds***—Hold-time value, in seconds.

Range: 1 through 65,535 seconds

Default: 180 seconds (three times the default hello interval)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

interface

Syntax interface (*interface-name* | all);

Hierarchy Level [edit protocols esis],
[edit routing-instances *routing-instance-name* protocols esis]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure ES-IS on an interface.

Options ***interface-name***—Name of the interface.

all—Configure on all interfaces.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

global-mac-limit

Syntax
```
global-mac-limit limit {
   packet-action drop;
}
```

Hierarchy Level [edit protocols l2-learning]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Limit the number of media access control (MAC) addresses learned from the logical interfaces on the router.

Default 131071 MAC addresses

Options ***limit***—Number of MAC addresses that can be learned on the device.
Range: 20 through 131071 addresses

The remaining statement is explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

 Copyright © 2011, Juniper Networks, Inc.

global-mac-table-aging-time

Syntax global-mac-table-aging-time *seconds*;

Hierarchy Level [edit protocols l2-learning]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Configure the timeout interval for entries in the MAC table.

Default 300 seconds

Options ***seconds***—Time elapsed before MAC table entries are timed out and entries are deleted from the table.

Range: 10 through 64000 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

global-no-mac-learning

Syntax global-no-mac-learning;

Hierarchy Level [edit protocols l2-learning]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Disable MAC learning for the entire device.

Default MAC learning is enabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

l2-learning

Syntax

```
l2-learning {
   global-mac-limit limit {
   packet-action-drop
   }
   global-mac-table-aging-time seconds;
   global-no-mac-learning;
}
```

Hierarchy Level [edit protocols]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Configure Layer 2 address learning and forwarding properties globally.

The statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

packet-action

Syntax packet-action drop;

Hierarchy Level [edit protocols l2-learning global-mac-limit *limit*]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Specify that packets for new source MAC addresses be dropped after the MAC address limit is reached.

Default Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

preference

Syntax preference *preference*;

Hierarchy Level [edit protocols esis],
[edit routing-instances *routing-instance-name* protocols esis]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the ES-IS preference value.

Options ***preference***—Preference value.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

[edit protocols esis],
[edit routing-instances *routing-instance-name* protocols esis]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure ES-IS protocol-level tracing options.

To specify more than one tracing operation, include multiple flag statements.

Default

The default ES-IS protocol-level tracing options are those inherited from the routing protocols **traceoptions** statement included at the **[edit routing-options]** hierarchy level.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

file ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place ES-IS tracing output in the file **esis-log**.

files ***number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 2 files

flag—Tracing operation to perform. To specify more than one flag, include multiple **flag** statements.

ES-IS Tracing Flags

- **error**—Errored ES-IS packets
- **esh**—End-System hello packets
- **graceful-restart**—Graceful restart events
- **ish**—Intermediate-System hello packets

Copyright © 2011, Juniper Networks, Inc.

Global Tracing Flags

- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations, including adjacency changes

Default: If you do not specify this option, only unusual or abnormal operations are traced.

- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

no-world-readable—(Optional) Prevent any user from reading the log file.

size *maximum-file-size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 15

Routing-Instances Hierarchy

This section contains the following topics:

- Routing-Instances Configuration Statement Hierarchy on page 239

Routing-Instances Configuration Statement Hierarchy

Use the statements in the **routing-instances** configuration hierarchy to configure routing instances.

```
routing-instances {
  routing-instance-name {
    description text ;
    forwarding-options{
      accounting group-name {
        output {
          aggregate-export-interval seconds ;
          cflowd hostname {
            aggregation {
              autonomous-system;
              destination-prefix;
              protocol-port;
              source-destination-prefix {
                caida-compliant;
              }
              source-prefix;
            }
            autonomous-system-type (origin | peer);
            port port-number ;
            version number ;
          }
        }
      }
      family {
        inet {
          filter (input input-filter-name | output output-filter-name );
        }
        inet6 {
          filter (input input-filter-name | output output-filter-name );
        }
        mpls {
          filter (input input-filter-name | output output-filter-name );
```

```
    }
  }
  helpers {
    bootp {
      client-response-ttl value ;
      description text ;
      interface interface-name {
        client-response-ttl value ;
        description text ;
        maximum-hop-count number ;
        minimum-wait-time seconds ;
        no-listen;
        server address {
          routing-instance [ value ];
        }
        vpn;
      }
      maximum-hop-count number ;
      minimum-wait-time seconds ;
      relay-agent-option;
      server address {
        routing-instance [ value ];
      }
      vpn;
    }
    domain {
      description text ;
      interface interface-name {
        description text ;
        no-listen;
        server address {
          routing-instance [ value ];
        }
      }
      server address {
        routing-instance [ value ];
      }
    }
    port port-number {
      description text ;
      interface interface-name {
        description text ;
        no-listen;
        server address {
          routing-instance [ value ];
        }
      }
      server address {
        routing-instance [ value ];
      }
    }
    tftp {
      description text ;
      interface interface-name {
        description text ;
        no-listen;
```

 Copyright © 2011, Juniper Networks, Inc.

```
            server address {
                routing-instance [ value ];
            }
        }
        server address {
            routing-instance [ value ];
        }
    }
    traceoptions {
        file filename <files number > <match regular-expression >
        <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag {
            address;
            all;
            bootp;
            config;
            domain;
            ifdb;
            io;
            main;
            port;
            rtsock;
            tftp;
            trace;
            ui;
            util;
        }
        level match-level ;
    }
}
packet-capture {
    disable;
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    maximum-capture-size size ;
}
sampling {
    disable;
    family (inet | inet6 | mpls ) {
        disable;
        output {
            extension-service name;
            file;
            flow-server name {
                aggregation {
                    source-destination;
                }
            }
        }
    }
    input {
        max-packets-per-second number;
        rate number ;
        run-length number ;
    }
```

```
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
  }
}
instance-type (forwarding | l2vpn | no-forwarding | virtual-router | vpls | vrf);
interface interface-name ;
multicast-snooping-options {
  flood-groups [ value ];
  forwarding-cache {
    threshold (suppress | reuse) value value ;
    timeout minutes ;
  }
  options {
    syslog {
      level level | upto level ;
      mark seconds;
    }
  }
}
no-local-switching;
no-vrf-advertise;
protocols {
  bgp {
    bgp-configuration ;
  }
  esis {
    esis-configuration ;
  }
  isis {
    isis-configuration ;
  }
  l2vpn {
    l2vpn-configuration ;
  }
  ldp {
    ldp-configuration ;
  }
  msdp {
    msdp-configuration;
  }
  ospf {
    domain-id domain-id ;
    domain-vpn-tag number ;
    route-type-community (vendor | iana);
    ospf-configuration ;
  }
  ospf3 {
    domain-id domain-id ;
    domain-vpn-tag number ;
    route-type-community (vendor | iana);
    ospf3-configuration ;
  }
  pim {
    mdt {
      group-range multicast-prefix ;
```

 Copyright © 2011, Juniper Networks, Inc.

```
            threshold {
              group group-address {
                source source-address {
                  rate threshold-rate ;
                }
              }
            }
            tunnel-limit limit ;
          }
          pim-configuration ;
        }
        rip {
          rip-configuration ;
        }
        router-discovery {
          router-discovery-configuration ;
        }
      }
      provider-tunnel {
        pim-asm {
          group-address group-address ;
        }
        rsvp-te {
          label-switched-path-template (default | lsp-template-name );
          static-lsp p2mp-lps-name ;
        }
        selective {
          group group-prefix ;
          tunnel-limit number ;
        }
      }
      route-distinguisher ( as-number : number | ip-address : number );
      routing-options {
        aggregate {
          defaults {
            aggregate-options ;
          }
          route destination-prefix {
            aggregate-options ;
            policy policy-name ;
          }
        }
        auto-export {
          (disable | enable);
          family {
            inet {
              disable;
              flow {
                (disable | enable);
                rib-group rib-group ;
              }
              multicast {
                (disable | enable);
                rib-group rib-group ;
              }
              unicast {
```

```
            (disable | enable);
            rib-group rib-group ;
          }
        }
        inet6 {
          disable;
          multicast {
            (disable | enable);
            rib-group rib-group ;
          }
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
        iso {
          disable;
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
      }
      traceoptions {
        file filename <files number >
        <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    autonomous-system autonomous-system <loops number > {
      independent-domain;
    }
    fate-sharing {
      group group-name {
        cost value ;
        from address {
          to address ;
        }
      }
    }
    flow {
      route name {
        match {
          match-conditions ;
        }
        then {
          actions ;
        }
      }
      validation {
        traceoptions {
          file filename <files number >
          <size maximum-file-size >
          <world-readable | no-world-readable>;
          flag flag < flag-modifier > <disable>;
```


Copyright © 2011, Juniper Networks, Inc.

```
      }
    }
  }
  forwarding-table {
    unicast-reverse-paths (active-paths | feasible-paths);
  }
  generate {
    defaults {
      generate-options ;
    }
    route destination-prefix {
      generate-options ;
      policy policy-name ;
    }
  }
  graceful-restart {
    disable;
    restart-duration duration ;
  }
  instance-export [ policy-names ];
  instance-import [ policy-names ];
  interface-routes {
    family (inet | inet6) {
      import [ import-policies ];
      export {
        lan;
        point-to-point;
      }
    }
    rib-group {
      inet group-name ;
      inet6 group-name ;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths path-limit <log-only | threshold value log-interval seconds >;
  maximum-prefixes prefix-limit <log-only | threshold value log-interval seconds
    >;
  multicast {
    flow-map map-name {
      bandwidth value {
        adaptive;
      }
      forwarding-cache {
        timeout minutes {
          never;
        }
      }
      policy [ policy-name ];
      redundant-sources [ source-address ];
    }
    forwarding-cache {
      threshold (suppress | reuse) value value ;
      timeout minutes ;
```

```
    }
    interface interface-name {
      maximum-bandwidth limit ;
    }
    rpf-check-policy [ value ];
    scope scope-name {
      interface [ interface-name ];
      prefix destination-prefix ;
    }
    scope-policy [ policy-name ];
    ssm-groups [ addresses ];
    ssm-map map-name {
      policy [ policy-name ];
      source [ source-address ];
    }
  }
  multipath {
    vpn-unequal-cost {
      equal-external-internal;
    }
  }
  options {
    mark seconds ;
    syslog (level level | upto level );
  }
  resolution {
    rib routing-table-name {
      import [ policy-names ];
      resolution-ribs [ routing-table-names ];
    }
  }
  rib routing-table-name {
    aggregate {
      defaults {
        aggregate-options ;
      }
      route destination-prefix {
        aggregate-options ;
        policy policy-name ;
      }
    }
    generate {
      defaults {
        generate-options ;
      }
      route destination-prefix {
        generate-options ;
        policy policy-name ;
      }
    }
    martians {
      destination-prefix match-type <allow>;
    }
    maximum-paths path-limit <log-only | threshold value log-interval seconds
      >;
    maximum-prefixes prefix-limit <log-only | threshold value log-interval
```

 Copyright © 2011, Juniper Networks, Inc.

```
    seconds >;
    multipath {
      vpn-unequal-cost {
        equal-external-internal;
      }
    }
    static {
      defaults {
        static-options ;
      }
      rib-group group-name ;
      route destination-prefix {
        bfd-liveness-detection {
          detection-time {
            threshold milliseconds ;
          }
          holddown-interval milliseconds;
          local-address ip-address ;
          minimum-interval milliseconds ;
          minimum-receive-interval milliseconds ;
          minimum-receive-ttl milliseconds ;
          multiplier number ;
          neighbor address ;
          transmit-interval {
            minimum-interval milliseconds ;
            threshold milliseconds ;
          }
          version (0 | 1);
        }
        lsp-next-hop nexthop {
          metric metric ;
          preference preference ;
        }
        next-hop [ nexthop ];
        qualified-next-hop ( address | interface-name ) {
          interface interface-name ;
          metric metric ;
          preference preference ;
        }
        static-options ;
      }
    }
  }
  router-id address ;
  static {
    defaults {
      static-options ;
    }
    rib-group group-name ;
    route destination-prefix {
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds ;
        }
        holddown-interval milliseconds;
        local-address ip-address ;
```

```
                minimum-interval milliseconds ;
                minimum-receive-interval milliseconds ;
                minimum-receive-ttl milliseconds ;
                multiplier number ;
                neighbor address ;
                transmit-interval {
                  minimum-interval milliseconds ;
                  threshold milliseconds ;
                }
                version (0 | 1);
              }
              lsp-next-hop nexthop {
                metric metric ;
                preference preference ;
              }
              next-hop [ nexthop ];
              qualified-next-hop ( address | interface-name ) {
                interface interface-name ;
                metric metric ;
                preference preference ;
              }
              static-options ;
            }
          }
        }
        vlan-id (all | none | vlan-id );
        vlan-tags {
          inner vlan-id ;
          outer vlan-id ;
        }
        vrf-export [ policy-names ];
        vrf-import [ policy-names ];
        vrf-table-label;
        vrf-target {
          export community-name ;
          import community-name ;
        }
      }
    }
  }
```

Related Documentation

- *Junos OS Design and Implementation Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Services Interfaces Configuration Guide*
- *Junos OS Multicast Protocols Configuration Guide*
- *Junos OS Network Interfaces Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 16

Routing-Options Hierarchy

This section contains the following topics:

- Routing-Options Configuration Statement Hierarchy on page 249

Routing-Options Configuration Statement Hierarchy

Use the statements in the **routing-options** configuration hierarchy to configure protocol-independent routing properties.

```
routing-options {
  aggregate {
    defaults {
      aggregate-options ;
    }
    route destination-prefix {
      policy policy-name ;
      aggregate-options ;
    }
  }
  auto-export {
    (disable | enable);
    family {
      inet {
        disable;
        flow {
          (disable | enable);
          rib-group rib-group ;
        }
        multicast {
          (disable | enable);
          rib-group rib-group ;
        }
        unicast {
          (disable | enable);
          rib-group rib-group ;
        }
      }
      inet6 {
        disable;
        multicast {
          (disable | enable);
```

```
            rib-group rib-group ;
          }
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
        iso {
          disable;
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    autonomous-system autonomous-system <loops number >;
    bgp-orf-cisco-mode;
    confederation confederation-autonomous-systems {
      members [ autonomous-system ] ;
    }
    dynamic-tunnels {
      tunnel-name {
        destination-networks prefix ;
        source-address address ;
        tunnel-type type-of-tunnel ;
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    fate-sharing {
      group group-name {
        cost value ;
        from address {
          to address ;
        }
      }
    }
    flow {
      route name {
        match {
          match-conditions ;
        }
        then {
          actions ;
        }
      }
      validation {
```


Copyright © 2011, Juniper Networks, Inc.

```
      traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
  }
  forwarding-table {
    export [ policy-names ];
    (indirect-next-hop | no-indirect-next-hop);
    unicast-reverse-paths (active-paths | feasible-paths);
  }
  generate {
    defaults {
      generate-options ;
    }
    route destination-prefix {
      policy policy-name ;
      generate-options ;
    }
  }
  graceful-restart {
    disable;
    restart-duration duration ;
  }
  instance-export [ policy-names ];
  instance-import [ policy-names ];
  interface-routes {
    family (inet | inet6) {
      import [ import-policies ];
      export {
        lan;
        point-to-point;
      }
    }
    rib-group {
      inet group-name ;
      inet6 group-name ;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths path-limit <log-only | threshold value log-interval seconds >;
  maximum-prefixes prefix-limit <log-only | threshold value log-interval seconds >;
  multicast {
    flow-map map-name {
      bandwidth value {
        adaptive;
      }
      forwarding-cache {
        timeout minutes {
          never;
        }
      }
      policy [ policy-name ];
```

```
        redundant-sources [ source-address ];
      }
      forwarding-cache {
        threshold (suppress | reuse) value value ;
        timeout minutes ;
      }
      interface interface-name {
        maximum-bandwidth limit ;
      }
      rpf-check-policy [ value ];
      scope scope-name {
        interface [ interface-name ];
        prefix destination-prefix ;
      }
      scope-policy [ policy-name ];
      ssm-groups [ addresses ];
      ssm-map map-name {
        policy [ policy-name ];
        source [ source-address ];
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    options {
      mark seconds ;
      syslog (level level | upto level );
    }
    resolution {
      rib routing-table-name {
        import [ policy-names ];
        resolution-ribs [ routing-table-names ];
      }
      tracefilter [ policy-name ];
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    rib routing-table-name {
      aggregate {
        defaults {
          aggregate-options ;
        }
        route destination-prefix {
          policy policy-name ;
          aggregate-options ;
        }
      }
      generate {
        defaults {
          generate-options ;
        }
```

 Copyright © 2011, Juniper Networks, Inc.

```
    route destination-prefix {
      policy policy-name ;
      generate-options ;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths path-limit <log-only | threshold value log-interval seconds >;
  maximum-prefixes prefix-limit <log-only | threshold value log-interval
  seconds >;
  static {
    defaults {
      static-options ;
    }
    rib-group group-name ;
    route destination-prefix {
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds ;
        }
        holddown-interval milliseconds;
        local-address ip-address ;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        minimum-receive-ttl milliseconds ;
        multiplier number ;
        neighbor address ;
        transmit-interval {
          minimum-interval milliseconds ;
          threshold milliseconds ;
        }
        version (0 | 1);
      }
      lsp-next-hop nexthop '{
        metric metric ;
        preference preference ;
      }
      next-hop [ next-hop ];
      qualified-next-hop ( address | interface-name ) {
        interface interface-name ;
        metric metric ;
        preference preference ;
      }
      static-options ;
    }
  }
}
rib-groups {
  group-name {
    export-rib [ group-names ];
    import-policy [ policy-names ];
    import-rib [ group-names ];
  }
}
route-distinguished-id address ;
```

```
route-record;
router-id address ;
source-routing (ip | ipv6);
static {
  defaults {
    static-options ;
  }
  rib-group group-name ;
  route destination-prefix {
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      holddown-interval milliseconds;
      local-address ip-address ;
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      minimum-receive-ttl milliseconds ;
      multiplier number ;
      neighbor address ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
      }
      version (0 | 1);
    }
    lsp-next-hop nexthop '{
      metric metric ;
      preference preference ;
    }
    next-hop [ next-hop ];
    qualified-next-hop ( address | interface-name ) {
      interface interface-name ;
      metric metric ;
      preference preference ;
    }
    static-options ;
  }
}
topologies {
  family (inet | inet6) {
    topology topology-name;
  }
}
traceoptions {
  file name <files number > <size maximum-file-size >
  <world-readable | no-world-readable>;
  flag flag < flag-modifier > <disable>;
}
}
```

Related Documentation

- *Junos OS Design and Implementation Guide*
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2011, Juniper Networks, Inc.

- *Junos OS Services Interfaces Configuration Guide*
- *Junos OS Multicast Protocols Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 17

Schedulers Hierarchy and Statements

This section contains the following topics:

- Schedulers Configuration Statement Hierarchy on page 257

Schedulers Configuration Statement Hierarchy

Use the statements in the **schedulers** configuration hierarchy to determine the day and time when security policies are in effect.

```
schedulers {
  scheduler scheduler-name {
    daily (all-day | exclude | start-time time stop-time time);
    friday {
      (all-day | exclude | start-time time stop-time time);
    }
    monday {
      (all-day | exclude | start-time time stop-time time);
    }
    saturday {
      (all-day | exclude | start-time time stop-time time);
    }
    start-date date-time stop-date date-time;
    sunday {
      (all-day | exclude | start-time time stop-time time);
    }
    thursday {
      (all-day | exclude | start-time time stop-time time);
    }
    tuesday {
      (all-day | exclude | start-time time stop-time time);
    }
    wednesday {
      (all-day | exclude | start-time time stop-time time);
    }
  }
}
```

Related Documentation

- *Junos OS Security Configuration Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

all-day

Syntax **all-day;**

Hierarchy Level

[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Schedule the security policy to be in effect for an entire day.

NOTE: A schedule set for a specific time overrides a schedule set with the **all-day** statement. Use the **all-day** statement to specify that a security policy be in effect for the whole day

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

daily

Syntax

```
daily {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Schedule the security policy to be in effect every day of the week.

If you create a daily schedule with the **daily** statement and also use the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statement in the schedule, the parameters specified for a specific day (for example, Friday using the **friday** statement) override the schedule set with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

exclude

Syntax

exclude;

Hierarchy Level

[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Exclude a specified day from the schedule.

Use the **exclude** statement to exclude a day from a daily schedule created with the **daily** statement. You cannot use the **exclude** statement for a particular day unless it is in conjunction with the **daily** statement in a schedule.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

friday

Syntax

```
friday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Friday.

If you use the **friday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **friday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Friday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

monday

Syntax

```
monday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Monday.

If you use the **monday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **monday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Monday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

saturday

Syntax

```
saturday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Saturday.

If you use the **saturday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **saturday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Saturday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

scheduler

Syntax

```
scheduler scheduler-name {
  daily (all-day | exclude | start-time time stop-time time );
  friday {
    (all-day | exclude | start-time time stop-time time );
  }
  monday {
    (all-day | exclude | start-time time stop-time time );
  }
  saturday {
    (all-day | exclude | start-time time stop-time time );
  }
  start-date date-time stop-date date-time ;
  sunday {
    (all-day | exclude | start-time time stop-time time );
  }
  thursday {
    (all-day | exclude | start-time time stop-time time );
  }
  tuesday {
    (all-day | exclude | start-time time stop-time time );
  }
  wednesday {
    (all-day | exclude | start-time time stop-time time );
  }
}
```

Hierarchy Level [edit schedulers]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Create or modify a schedule that defines when security policies are in effect.

You configure a schedule to start at a specific date and time or start on a recurrent basis.

Options *scheduler-name* —Name of the schedule. The schedule name must consist of 1 to 63 characters that can be letters, numbers, dashes, and underscores and can begin with a number or letter.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

schedulers

Syntax **schedulers { ... }**

Hierarchy Level **[edit]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure schedules for security policies that allow you to control network traffic flow and enforce network security.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

start-date

Syntax **start-date** ***date-time*** **;**

Hierarchy Level **[edit schedulers],**
[edit schedulers scheduler ***scheduler-name*** **]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time, day, month, and year that the schedule starts.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

Options ***date-time*** —Use the format **[** ***yyyy*** **-]** ***mm*** **-** ***dd*** **.** ***hh*** **.** ***mm*** to specify the year, month, day, hour, and minutes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

start-time

Syntax **start-time** *time* ;

Hierarchy Level
[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time that a schedule starts for a specified day.

If you specify a starting time for a daily schedule with the **daily** statement and also include the the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the starting time specified for a specific day (for example, Friday using the **friday** statement) overrides the starting time set with the **daily** statement.

Options ***time*** —Use the 24-hour format (***hh*** : ***mm*** : ***ss***) to specify the hours, minutes, and seconds.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

stop-date

Syntax **stop-date** *date-time* **;**

Hierarchy Level **[edit schedulers],**
[edit schedulers scheduler *scheduler-name* **]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time, day, month, and year that the schedule ends.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

Options ***date-time*** —Use the format **[** *yyyy* **-]** *mm* **-** *dd* **.** *hh* **.** *mm* to specify the year, month, day, hour, and minutes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

stop-time

Syntax **stop-time** *time* ;

Hierarchy Level
[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time that a schedule stops for a specified day.

If you specify a stop time for a daily schedule with the **daily** statement and also include the the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the stop time specified for a specific day (for example, Friday using the **friday** statement) overrides the stop time set with the **daily** statement.

Options ***time*** —Use the 24-hour format (***hh*** : ***mm*** : ***ss***) to specify the hours, minutes, and seconds.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sunday

Syntax **sunday (all-day | exclude | start-time** *time* **stop-time** *time* **);**

Hierarchy Level **[edit schedulers scheduler** *scheduler-name* **]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a schedule for every Sunday.

If you use the **sunday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **sunday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Sunday from a daily schedule configured with the **daily** statement.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

thursday

Syntax

```
thursday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Thursday.

If you use the **thursday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **thursday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Thursday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

tuesday

Syntax

```
tuesday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Tuesday.

If you use the **tuesday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **tuesday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Tuesday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

wednesday

Syntax

```
wednesday {
   (all-day | exclude | start-time  time  stop-time  time  );
}
```

Hierarchy Level

[edit schedulers scheduler *scheduler-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify a schedule for every Wednesday.

If you use the **wednesday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **wednesday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Wednesday from a daily schedule configured with the **daily** statement.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 18

Security Hierarchy and Statements

This section contains the following topics:

- Security Configuration Statement Hierarchy on page 273
- no-allow-icmp-without-flow on page 587
- no-enable-all-qmodules on page 588
- no-enable-packet-pool on page 588
- no-log-errors on page 588
- no-policy-lookup-cache on page 590
- no-reset-on-policy on page 590

Security Configuration Statement Hierarchy

Use the statements in the **security** configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, Unified Threat Management (UTM), and zones. Statement descriptions that are exclusive to the Juniper Networks devices running Junos OS are described in this section.

```
security {
  alg {
    dns {
      disable;
      maximum-message-length number;
      traceoptions {
        flag {
          all <extensive>;
        }
      }
    }
    ftp {
      disable;
      traceoptions {
        flag {
          all <extensive>;
```

```
        }
      }
    }
    h323 {
      application-screen {
        message-flood {
          gatekeeper threshold rate;
        }
        unknown-message {
          permit-nat-applied;
          permit-routed;
        }
        disable;
        endpoint-registration-timeout seconds;
        media-source-port-any;
        traceoptions {
          flag {
            all <detail | extensive | terse>;
            cc <detail | extensive | terse>;
            h225-asn1 <detail | extensive | terse>;
            h245 <detail | extensive | terse>;
            h245-asn1 <detail | extensive | terse>;
            q931 <detail | extensive | terse>;
            ras <detail | extensive | terse>;
            ras-asn1 <detail | extensive | terse>;
          }
        }
      }
      dscp-rewrite {
        code-point 6 bit patterns;
      }
    }
    ike-esp-nat {
      enable;
      state-timeout timeout-in-seconds;
      esp-gate-timeout timeout-in-seconds;
      esp-session-timeout timeout-in-seconds;
    }
    mgcp {
      application-screen {
        connection-flood threshold rate;
        message-flood threshold rate;
        unknown-message {
          permit-nat-applied;
          permit-routed;
        }
      }
      disable;
      dscp-rewrite {
        code-point 6 bit patterns;
      }
      inactive-media-timeout seconds;
      maximum-call-duration minutes;
      traceoptions {
        flag {
          all <extensive>;
```


Copyright © 2011, Juniper Networks, Inc.

```
            call <extensive>;
            cc <extensive>;
            decode <extensive>;
            error <extensive>;
            nat <extensive>;
            packet <extensive>;
            rm <extensive>;
        }
    }
    transaction-timeout seconds;
}
msrpc {
    disable;
    traceoptions {
        flag {
            all <extensive>
        }
    }
}
pptp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
real {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
rsh {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
rtsp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
sccp {
    application-screen {
        call-flood threshold rate;
        unknown-message {
            permit-nat-applied;
```

```
            permit-routed;
          }
        }
        disable;
        dscp-rewrite {
          code-point 6 bit patterns;
        }
        inactive-media-timeout seconds;
        traceoptions {
          flag {
            all <extensive>;
            call <extensive>;
            cc <extensive>;
            cli <extensive>;
            decode <extensive>;
            error <extensive>;
            init <extensive>;
            nat <extensive>;
            rm <extensive>;
          }
        }
      }
      sip {
        application-screen {
          protect {
            deny {
              all | destination-ip address;
              timeout seconds;
            }
          }
          unknown-message {
            permit-nat-applied;
            permit-routed;
          }
        }
        c-timeout minutes;
        disable;
        dscp-rewrite {
          code-point 6 bit patterns;
        }
        disable-call-id-hiding;
        inactive-media-timeout seconds;
        maximum-call-duration  minutes;
        retain-hold-resource;
        t1-interval milliseconds;
        t4-interval seconds;
        traceoptions {
          flag {
            all <detail | extensive | terse>;
            call <detail | extensive | terse>;
            cc <detail | extensive | terse>;
            nat <detail | extensive | terse>;
            parser <detail | extensive | terse>;
            rm <detail | extensive | terse>;
          }
        }
```


Copyright © 2011, Juniper Networks, Inc.

```
        }
        sql {
          disable;
          traceoptions {
            flag {
              all <extensive>;
            }
          }
        }
        sunrpc {
          disable;
          traceoptions {
            flag {
              all <extensive>;
            }
          }
        }
        talk {
          disable;
          traceoptions {
            flag {
              all <extensive>;
            }
          }
        }
        tftp {
          disable;
          traceoptions {
            flag {
              all <extensive>;
            }
          }
        }
    analysis no-reports;
      application-firewall {
        rule-sets {
          rule-set-name {
            rule rule-name {
              match {
                dynamic-application [dynamic-application-names];
              }
              then {
                permit | deny;
              }
            }
            default-rule {
              permit | deny;
            }
          }
        }
        traceoptions {
          file filename {
            <files number>;
            <match regular-expression>;
            <size maximum-file-size >;
            <world-readable | no-world-readable>;
```

```
        }
        flag {
          all;
          compilation;
          configuration;
          ipc;
          lookup;
        }
        no-remote-trace;
      }
    }
    application-tracking {
      first-update;
      first-update-interval number;
      session-update-interval number;
    }
    dynamic-vpn {
      access-profileprofile-name;
      force-upgrade;
      clients {
        configuration-name {
          remote-protected-resources{
            ip-address/mask;
          }
          remote-exceptions{
            ip-address/mask;
          }
          ipsec-vpn configuration-name;
          user{
            username;
          }
        }
      }
    }
    datapath-debug{
      action-profile{
        event (jexec | lbt | mac-egress | mac-ingress | np-egress | np-ingress | pot)
          {
            count;
            packet-dump;
            packet-summary;
            trace;
          }
          module{
            flow{
              flag{
                all;
              }
            }
          }
          preserve-trace-order;
          record-pic-history;
      capture—file;
      packet—filter
        {
          action-profile (action-profile name| default) ;
```


Copyright © 2011, Juniper Networks, Inc.

```
            destination-port (port-range| protocol name);
            destination-prefix destination-prefix
            protocol (protocol number | (ah | egp | esp | gre | icmp | igmp | ipip | ospf | pim |
              rsvp | sctp | tcp | udp));
            source-port (port-range| protocol name);
            source-prefix source-prefix;
          }
        trace-options
          {
          file
            {
              filename;
              files filesnumber;
              match regular expression;
              size maximum file-size;
              (world-readable | no-world-readable);
            }
          no-remote-trace;
        }
      }
      firewall-authentication {
        traceoptions {
          flag {
            all <detail | extensive | terse>;
            authentication <detail | extensive | terse>;
            proxy <detail | extensive | terse>;
          }
        }
      }
      flow {
        aging {
          early-ageout seconds;
          high-watermark percent;
          low-watermark percent;
        }
        allow-dns-reply;
        bridge {
          block-non-ip-all;
          bypass-non-ip-unicast;
          no-packet-flooding {
            no-trace-route;
          }
        }
        route-change-timeout seconds;
        syn-flood-protection-mode (syn-cookie | syn-proxy);
        tcp-mss {
          all-tcp {
            mss value;
          }
          gre-in {
            mss  value;
          }
          gre-out {
            mss  value;
          }
          ipsec-vpn {
```

```
            mss value;
        }
    }
    tcp-session {
        no-sequence-check;
        no-syn-check;
        no-syn-check-in-tunnel;
        rst-invalidate-session;
        rst-sequence-check;
        tcp-initial-timeout seconds;
    }
    traceoptions {
        file filename <files number > <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
    }
}
forwarding-options {
    family {
        inet6 {
            mode (packet-based | flow-based | drop ); default: drop
        }
        iso {
            mode packet-based;
        }
        mpls {
            mode packet-based;
        }
    }
}
forwarding-process {
    application-services {
        maximize-alg-sessions;
        maximize-cp-sessions;
        maximize-idp-sessions {
            inline-tap;
            weight {
                equal;
                firewall;
                idp;
            }
        }
    }
gprs {
    gtp {
        enable;
        profile profile name {
            apn pattern-string {
                mcc-mnc <mcc-mnc-number> {
                    action <drop | pass | selection <ms | net | vrf> {
                        }
                    }
            drop {
            aa-create-pdp {
                <0 | 1 | All>;
            }
```


Copyright © 2011, Juniper Networks, Inc.

```
aa-delete-pdp {
   <0 | 1 | All>;
}
create pdp {
   <0 | 1 | All>;
}
data-record {
   <0 | 1 | All>;
}
delete-pdp {
   <0 | 1 | All>;
}
echo {
   <0 | 1 | All>;
}
error-indication {
   <0 | 1 | All>;
}
failure-report {
   <0 | 1 | All>;
}
fwd-relocation {
   <0 | 1 | All>;
}
fwd-srns-context {
   <0 | 1 | All>;
}
g-pdu {
   <0 | 1 | All>;
}
identification {
   <0 | 1 | All>;
}
node-alive {
   <0 | 1 | All>;
}
note-ms-present {
   <0 | 1 | All>;
}
pdu-notification {
   <0 | 1 | All>;
}
ran-info {
   <0 | 1 | All>;
}
redirection {
   <0 | 1 | All>;
}
relocation-cancel {
   <0 | 1 | All>;
}
send-route {
   <0 | 1 | All>;
}
sgsn-context {
   <0 | 1 | All>;
```

```
        }
        supported-extension {
          <0 | 1 | All>;
        }
        update-pdp {
          <0 | 1 | All>;
        }
        ver-not-supported {
          <0 | 1 | All>;
        }
        log {
          forwarded <basic | detail>;
          prohibited <basic | detail>;
          rate-limited <basic | detail>;
            frequency-number <number>;
            }
          state-invalid <basic | detail>;
        }
        max-message-length number;
        min-message-length number;
        rate-limit messages per second;
        remove-r6;
        seq-number-validated;
        timeout <number of hours>;
        }
      }
      traceoptions
        file filename {
          <files | match | no-world-readable | size | world-readable>;
          }
        flag {
          < all | chassis-cluster | configuration | flow | parser | >;
          }
        no-remote-trace;
    }
    sctp {
      log {
        configuration;
        decoding-error;
        dropped-packet;
        exceeding-rate-limit;
      }
      profile name {
        association-timeout time in minutes;
        handshake-timeout time in seconds;
        drop {
          m3ua-service {
            isup;
            sccp;
            tup;
          }
          payload-protocol {
            all;
            asap;
            bicc;
            ddp-segment;
```

 Copyright © 2011, Juniper Networks, Inc.

```
                ddp-stream;
                dua;
                enrp;
                h248;
                h323;
                iua;
                m2pa;
                m2ua;
                m3ua;
                qipc;
                simco;
                sua;
                tali;
                v5ua;
              }
            }
            limit {
              rate {
                address ip-address {
                  sccp number;
                  ssp number;
                  sst number;
                }
                sccp number;
                ssp number;
                sst number;
              }
            }
          }
          traceoptions {
            file;
            flag {
              all;
              chassis-cluster;
              configuration;
              flow;
              parser;
            }
          }
        }
      }
      group-vpn {
        co-location;
        member {
          ike {
            gateway gateway-name {
              address [( ip-address | hostname )] |
              dead-peer-detection {
                always-send;
                interval seconds ;
                threshold number ;
              }
              dynamic {
                connections-limit number;
                  distinguished-name {
                  container container-string;
```

```
                wildcard wildcard-string;
                }
                hostname domain-name;
                ike-user-type (group-ike-id | shared-ike-id);
                inet ip-address;
                inet6 ipv6-address;
              user-at-hostname user-at-hostname;
            external-interface external-interface-name ;
            ike-policy name ;
            local-address address;
            local-identity (distinguished-name string | hostname hostname | inet ip-address
              |
            user-at-hostname e-mail-address | distinguished-name string );
            nat-keepalive seconds ;
            no-nat-traversal;
            xauth {
              access-profile profile-name ;
            }
          }
          policy name {
            certificate {
              local-certificate identifier;
              peer-certificate-type [pkcs7 | x509-signature);
              trusted-ca (ca-index | use-all);
            }
            description text;
            mode (aggressive | main);
            pre-shared-key (ascii-text text | hexadecimal hex);
            proposal-set (basic | compatible | standard);
            proposals name;
          }
          proposal name {
            authentication-algorithm (md5 | sha1 | sha-256);
            authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
            description text;
            dh-group (group1 | group2 | group5 | group 14);
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
              des-cbc);
            lifetime-seconds seconds;
          }
        }
        ipsec vpn name {
          group id;
          group-vpn-external-interface interface;
          heartbeat-threshold number;
          ike-gateway name;
        }
      }
      server {
        gateway gateway-name {
          address [( ip-address | hostname )] |
          dead-peer-detection {
            always-send;
            interval seconds ;
            threshold number ;
          }
```

 Copyright © 2011, Juniper Networks, Inc.

```
    dynamic {
      connections-limit number ;
      distinguished-name {
        container container-string ;
        wildcard wildcard-string ;
      }
      hostname domain-name ;
      ike-user-type (group-ike-id | shared-ike-id);
      inet ip-address ;
      inet6 ipv6-address ;
      user-at-hostname user-at-hostname ;
    }
    external-interface external-interface-name ;
    ike-policy name ;
    local-address address;
    local-identity (distinguished-name string | hostname hostname | inet ipv4-ip-address
      | inet6 ipv6-address| user-at-hostname e-mail-address);
    user-at-hostname e-mail-address | distinguished-name string );
    nat-keepalive seconds ;
    no-nat-traversal;
    xauth {
      access-profile profile-name ;
    }
  }
  group name{
    activation-time-delay seconds;
    anti-replay-time-window seconds;
    description text;
    group-id number;
    ike-gateway gateway-name;
    ipsec-sa name {
      proposal name;
        match-policy name {
          destination ip-address/netmask;
          destination-port number;
          protocol number;
          source ip-address/netmask;
          source-port number;
      }
    }
    no-anti-replay;
    server-address ip-address;
    server-member-communication {
      certificate certificate-id;
      communication-type (multicast | unicast);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
        des-cbc);
      heartbeat seconds;
      lifetime-seconds seconds;
      multicast-group address;
      multicast-outgoing-interface interface;
      number-of-retransmission number;
      retransmission-period seconds;
      sig-hash-algorithm (md5 | sha1);
    }
  }
```

```
ike {
  gateway gateway-name {
    address [( ip-address | hostname )] |
    dead-peer-detection {
      always-send;
      interval seconds ;
      threshold number ;
    }
    dynamic {
      connections-limit number ;
      distinguished-name {
        container container-string ;
        wildcard wildcard-string ;
      }
      hostname domain-name ;
      ike-user-type (group-ike-id | shared-ike-id);
      inet ip-address ;
      inet6 ipv6-address ;
      user-at-hostname user-at-hostname ;
    }
    external-interface external-interface-name ;
    ike-policy name ;
    local-identity (distinguished-name string | hostname hostname | inet
      ipv4-ip-address | inet6 ipv6-address| user-at-hostname e-mail-address);
    user-at-hostname e-mail-address | distinguished-name string );
    nat-keepalive seconds ;
    no-nat-traversal;
    xauth {
      access-profile profile-name ;
    }
  }
  policy name {
    certificate {
      local-certificate identifier;
      peer-certificate-type [pkcs7 | x509-signature);
      trusted-ca (ca-index | use-all);
    }
    description text;
    mode (aggressive | main);
    pre-shared-key (ascii-text text | hexadecimal hex);
    proposal-set (basic | compatible | standard);
    proposals name;
  }
  proposal name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description text;
    dh-group (group1 | group2 | group5 | group 14);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
      des-cbc);
    lifetime-seconds seconds;
  }
}
ipsec proposal name {
  authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
  description text;
```


Copyright © 2011, Juniper Networks, Inc.

```
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
              des-cbc);
            lifetime-seconds seconds;
          }
          traceoptions {
            file {
              files number;
              match regexp;
              (no-world-readable | world-readable);
              size size;
            }
            flag {
              all | certificates | config | database | general | high-availability | ike
              | next-hop-tunnels | parse | policy-manager | routing-socket | thread | timer
            }
            no-remote-trace;
          }
        }
      }
      idp {
        active-policy policy-name;
        application-ddos <name> {
          connection-rate-threshold number;
          context <context-name> {
            exclude-context-values regular-expression;
            hit-rate-threshold number;
            max-context-values number;
            time-binding-count number;
            time-binding-period seconds;
            value-hit-rate-threshold seconds;
          }
          service <dns | http>;
        }
        custom-attack attack-name {
          attack-type {
              anomaly {
                direction (any | client-to-server | server-to-client);
                service service-name;
                shellcode (all | intel | no-shellcode | sparc);
                test test-condition;
              }
              chain {
                expression boolean-expression;
                member member-name {
                  attack-type {
                    (anomaly | signature);
                  }
                }
                order;
                protocol-binding {
                  application application-name;
                  icmp;
                  ip {
                    protocol-number transport-layer-protocol-number;
                  }
                  rpc {
```

```
            program-number rpc-program-number;
        }
        tcp {
            minimum-port port-number maximum-port port-number;
        }
        udp {
            minimum-port port-number maximum-port port-number;
        }
    }
    reset;
    scope (session | transaction);
}
signature {
    context context-name;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern;
    protocol {
        icmp {
            code {
                match (equal | greater-than | less-than | not-equal);
                value code-value;
            }
            data-length {
                match (equal | greater-than | less-than | not-equal);
                value data-length;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            sequence-number {
                match (equal | greater-than | less-than | not-equal);
                value sequence-number;
            }
            type {
                match (equal | greater-than | less-than | not-equal);
                value type-value;
            }
        }
        ip {
            destination {
                match (equal | greater-than | less-than | not-equal);
                value hostname;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            ip-flags {
                (df | no-df);
                (mf | no-mf);
                (rb | no-rb);
            }
            protocol {
                match (equal | greater-than | less-than | not-equal);
```


Copyright © 2011, Juniper Networks, Inc.

```
        value transport-layer-protocol-id;
      }
      source {
        match (equal | greater-than | less-than | not-equal);
        value hostname;
      }
      tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
      }
    }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
      }
      mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
      }
      option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
      }
      source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
      }
      tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
```

```
                (r1 | no-r1);
                (r2 | no-r2);
                (rst | no-rst);
                (syn | no-syn);
                (urg | no-urg);
              }
              urgent-pointer {
                match (equal | greater-than | less-than | not-equal);
                value urgent-pointer;
              }
              window-scale {
                match (equal | greater-than | less-than | not-equal);
                value window-scale-factor;
              }
              window-size {
                match (equal | greater-than | less-than | not-equal);
                value window-size;
              }
            }
            udp {
              data-length {
                match (equal | greater-than | less-than | not-equal);
                value data-length;
              }
              destination-port {
                match (equal | greater-than | less-than | not-equal);
                value destination-port;
              }
              source-port {
                match (equal | greater-than | less-than | not-equal);
                value source-port;
              }
            }
          }
          protocol-binding {
            application application-name;
            icmp;
            ip {
              protocol-number transport-layer-protocol-number;
            }
            rpc {
              program-number rpc-program-number;
            }
            tcp {
              minimum-port port-number maximum-port port-number;
            }
            udp {
              minimum-port port-number maximum-port port-number;
            }
          }
          regexp regular-expression;
          shellcode (all | intel | no-shellcode | sparc);
        }
      }
      recommended-action (close | close-client | close-server | drop | drop-packet | ignore
        | none);
```


Copyright © 2011, Juniper Networks, Inc.

```
    severity (critical | info | major | minor | warning);
    time-binding {
        count count-value;
        scope (destination | peer | source);
    }
}
custom-attack-group custom-attack-group-name {
    group-members [attack-group-name | attack-name];
}
dynamic-attack-group dynamic-attack-group-name {
    filters {
        category {
            values [list-of-values];
        }
        direction {
            values [any | client-to-server | exclude-any | exclude-client-to-server |
                exclude-server-to-client | server-to-client];
        }
        false-positives {
            values [frequently | occasionally | rarely | unknown];
        }
        performance {
            values [fast | normal | slow | unknown];
        }
        products {
            values [list-of-values];
        }
        recommended;
        service {
            values [list-of-values];
        }
        severity {
            values [critical | info | major | minor | warning];
        }
        type {
            values [anomaly | signature];
        }
    }
}
idp-policy policy-name {
    rulebase-ddos {
        rule rule-name {
            description text ;
            match {
                application [ any | default ];
                application-ddos ddos-application-name;
                destination-address [ address-name ];
                from-zone zone-name;
                source-address [ address-name ];
                to-zone zone-name;
            }
            then {
                action <close-server | drop-connection | drop-packet | no-action>;
                ip-action {
                    <ip-block | ip-close | ip–connection–rate-limit value | ip-notify | log>;
                    timeout secconds;
```

```
            }
        }
    }
}
rulebase-exempt {
    rule rule-name {
        description text;
        match {
            attacks {
                custom-attacks [attack-name];
                predefined-attack-groups [attack-name];
                predefined-attacks [attack-name];
            }
            destination-address [address-name];
            destination-except [address-name];
            from-zone zone-name;
            source-address [address-name];
            source-except [address-name];
            to-zone zone-name;
        }
    }
}
rulebase-ips {
    rule rule-name {
        description text;
        match {
            attacks {
                custom-attacks [ attack-name ];
                predefined-attack-groups [ attack-name ];
                predefined-attacks [ attack-name ];
            }
            destination-address [ address-name ];
            destination-except [ address-name ];
            from-zone zone-name;
            source-address [ address-name ];
            source-except [ address-name ];
            to-zone zone-name;
        }
        terminal;
        then {
            action {
                (close-client | close-client-and-server | close-server |
                drop-connection | drop-packet | ignore-connection |
                mark-diffserv value  | no-action | recommended);
            }
            ip-action {
                (ip-block | ip-close | ip-notify);
                log;
                target (destination-address | service | source-address |
                source-zone | zone-service);
                timeout seconds;
            }
            notification {
                log-attacks {
                    alert;
                }
```


Copyright © 2011, Juniper Networks, Inc.

```
                packet-log {
                  pre-attack number;
                  post-attack number;
                  post-attack-timeout seconds;
                }
              }
              severity (critical | info | major | minor | warning);
            }
          }
        }
      }
      security-package {
        automatic {
          download-timeout;
          enable;
          interval hours;
          start-time start-time;
        }
        url url-name;
      }
      sensor-configuration {
        application-identification {
          application-system-cache;
          application-system-cache-timeout value;
          disable;
          max-packet-memory value;
          max-sessions value;
          max-tcp-session-packet-memory value;
          max-udp-session-packet-memory value;
          no-application-system–cache;
        }
        application-ddos {
          statistics interval;
        }
        detector {
          protocol-name protocol-name {
            tunable-name tunable-name {
              tunable-value protocol-value;
            }
            ssl-inspection
          }
        }
        flow {
          (allow-icmp-without-flow | no-allow-icmp-without-flow);
          (log-errors | no-log-errors);
          max-timers-poll-ticks value;
          reject-timeout value;
          (reset-on-policy | no-reset-on-policy);
        }
        global {
          (enable-all-qmodules | no-enable-all-qmodules);
          (enable-packet-pool | no-enable-packet-pool);
          (policy-lookup-cache | no-policy-lookup-cache);
        }
        ips {
          detect-shellcode;
```

```
            ignore-regular-expression;
            log-supercede-min minimum-value;
            pre-filter-shellcode;
            process-ignore-s2c;
            process-override;
            process-port port-number;
        }
        log {
            cache-size size;
            suppression {
                disable;
                include-destination-address;
                max-logs-operate value;
                max-time-report value;
                start-log value;
            }
        }
        packet-log {
            total-memory percentage;
            max-sessions percentage;
            source-address ip-address;
            host ip-address port number;
        }
        re-assembler {
            ignore-mem-overflow;
            max-flow-mem value;
            max-packet-mem value;
        }
        ssl-inspection {
            sessions number;
        }
    }
    traceoptions {
        file filename {
            <files number>;
            <match regular-expression>;
            <size maximum-file-size>;
            <world-readable | no-world-readable>;
        }
        flag all;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
ike {
    gateway gateway-name {
        address [( ip-address | hostname )] |
        dead-peer-detection {
            always-send;
            interval seconds ;
            threshold number ;
        }
        dynamic {
            connections-limit number;
                distinguished-name {
                container container-string;
```


Copyright © 2011, Juniper Networks, Inc.

```
            wildcard wildcard-string;
            }
            hostname domain-name;
            ike-user-type (group-ike-id | shared-ike-id);
            inet ip-address;
            inet6 ipv6-address;
        user-at-hostname user-at-hostname;
    external-interface external-interface-name ;
    ike-policy name ;
    local-address address;
    local-identity (distinguished-name string | hostname hostname | inet ip-address
        |
    user-at-hostname e-mail-address | distinguished-name string );
    nat-keepalive seconds ;
    no-nat-traversal;
    xauth {
        access-profile profile-name ;
    }
}
policy policy-name {
    certificate {
        local-certificate certificate-id;
        peer-certificate-type (pkcs7 | x509-signature);
        trusted-ca (ca-index | use-all);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text | hexadecimal);
    proposal-set (basic | compatible | standard);
    proposals [proposal-names];
}
proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2 | group5 | group14);
    encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
    | aes-256-cbc);
    lifetime-seconds seconds;
}
respond-bad-spi number;
traceoptions {
    file filename {
        <files number>;
        <match regular-expression>;
        <size maximum-file-size>;
    }
    flag {
        all;
        certificates;
        database;
        general;
        ike;
        parse;
        policy-manager;
        routing-socket;
```

```
            timer;
            snmp;
        }
    }
}
ipsec {
    policy policy-name {
        description description;
        perfect-forward-secrecy keys (group1 | group2 | group5 | group14);
        proposal-set (basic | compatible | standard);
    }
    proposal proposal-name {
        description description;
        encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
        | aes-256-cbc);
        lifetime-kilobytes kilobytes;
        lifetime-seconds seconds;
        protocol (ah | esp);
    }
    traceoptions {
        flag {
            all;
            next-hop-tunnel-binding;
            packet-drops;
            packet-processing;
            security-associations;
        }
    }
    vpn vpn-name {
        bind-interface interface-name;
        df-bit (clear | copy | set);
        establish-tunnels (immediately | on-traffic);
        ike {
            gateway gateway-name;
            idle-time seconds;
            install-interval seconds;
            ipsec-policy ipsec-policy-name;
            no-anti-replay;
            proxy-identity {
                local ip-prefix;
                remote ip-prefix;
                service service-name;
            }
        }
        manual {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key);
            }
            authentication-key-chains {
                key-chain key-chain-name {
                    description text ;
                    tolerance seconds ;
                }
            }
            encryption {
```


Copyright © 2011, Juniper Networks, Inc.

```
            algorithm (3des-cbc | aes-128-cbc | aes-192-cbc
            | aes-256-cbc | des-cbc);
            key (ascii-text key | hexadecimal key);
          }
          external-interface external-interface-name;
          gateway ip-address;
          protocol (ah | esp);
          spi spi value;
        }
        vpn-monitor {
          destination-ip ip-address;
          optimized;
          source-interface interface-name;
        }
      }
      vpn-monitor-options {
        interval seconds;
        threshold number;
      }
    }
    log {
      mode (event | stream);
      event-rate rate;
      format (syslog | sd-syslog) ;
      stream stream-name format (syslog | sd-syslog | welf) category (all | content-security)
        host ip-address;
      traceoptions {
        file filename;
        files number;
          match regular-expression;
          size maximum-file-size;
          (world-readable | no-world-readable);
        }
        flag (all | configuration | source);
      no-remote-trace;
    }
    nat {
      destination {
        pool pool-name {
          address <ip-address> (to ip-address | port port-number):
          routing-instance routing-instance-name;
        }
        rule-set rule-set-name {
          from interface [interface-name] |
          routing-instance [routing-instance-name] | zone [zone-name];
          rule rule-name {
            match {
              destination-address destination-address;
              destination-port port-number;
              source-address [source-address];
            }
            then {
              destination-nat (off | pool pool-name);
            }
          }
        }
```

```
}
proxy-arp {
   interface interface-name {
      address ip-address to ip-address;
   }
}
source {
   address-persistent;
   interface {
      port-overloading { off };
   }
   pool pool-name {
      address ip-address to ip-address;
      host-address-base ip-address;
      overflow-pool (interface | pool-name);
      port no-translation | range high ip-address low ip-address;
      routing-instance routing-instance-name;
   }
   pool-utilization-alarm {
      clear-threshold threshold-value;
      raise-threshold threshold-value;
   }
   port-randomization {
      disable;
   }
   rule-set rule-set-name {
      from interface [interface-name] |
      routing-instance [routing-instance-name] | zone [zone-name];
      rule rule-name {
         match {
            destination-address [destination-address];
            destination-port port-number;
            source-address [source-address];
         }
         then {
            source-nat (off | interface | pool pool-name);
            persistent-nat {
               address-mapping;
               inactivity-timeout seconds;
               max-session-number number;
               permit ( any-remote-host | target-host | target-host-port );
            }
         }
      }
      to interface [interface-name] |
      routing-instance [routing-instance-name] | zone [zone-name];
   }
}
static {
   rule-set rule-set-name {
      from interface [interface-name] |
      routing-instance [routing-instance-name] | zone [zone-name];
      rule rule-name {
         match {
            destination-address [destination-address];
         }
```


Copyright © 2011, Juniper Networks, Inc.

```
            then {
                static-nat prefix <addr-prefix>
                <routing-instance routing-instance-name>;
            }
        }
    }
}
traceoptions {
    file filename {
        <files number>;
        <match regular-expression>;
        <size maximum-file-size>;
        <world-readable | no-world-readable>;
    }
    flag {
        all;
        destination-nat-pfe;
        destination-nat-re;
        destination-nat-rt;
        source-nat-pfe;
        source-nat-re;
        source-nat-rt;
        static-nat-pfe;
        static-nat-re;
        static-nat-rt;
    }
    no-remote-trace;
}
}
pki {
    auto-re-enrollment {
        certificate-id certificate-id-name {
            ca-profile-name ca-profile-name;
            challenge-password password;
            re-enroll-trigger-time-percentage percentage;
            re-generate-keypair;
        }
    }
    ca-profile ca-profile-name {
        administrator {
            e-mail-address e-mail-address;
        }
        ca-identity ca-identity;
        routing-instance routing-instance-name;
        enrollment {
            retry number;
            retry-interval seconds ;
            url url-name;
        }
        revocation-check {
            crl {
                disable {
                    on-download-failure;
                }
                refresh-interval hours;
                url url-name;
```

```
            }
            disable;
        }
    }
    traceoptions {
        file filename <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
    }
}
policies {
    default-policy {
        (deny-all | permit-all);
    }
    from-zone zone-name to-zone zone-name {
        policy policy-name {
            match {
                application [application-name-or-set];
                destination-address {
                    address-name ;
                }
                source-address {
                    address-name ;
                }
            }
            scheduler-name scheduler-name;
            then {
                count {
                    alarm {
                        per-minute-threshold number;
                        per-second-threshold number;
                    }
                }
                (deny | reject);
                permit {
                    application-services {
                        application-firewall {
                            rule-set rule-set-name;
                        }
                    }
                    destination-address {
                        drop-translated;
                        drop-untranslated;
                    }
                    firewall-authentication {
                        pass-through {
                            access-profile profile-name>;
                            client-match match-name>;
                            web-redirect;
                        }
                        web-authentication {
                            client-match user-or-group;
                        }
                    }
                    tunnel {
                        ipsec-group-vpn group-vpn;
```

 Copyright © 2011, Juniper Networks, Inc.

```
                ipsec-vpn vpn-name;
                pair-policy pair-policy;
              }
            }
            log {
              session-close;
              session-init;
            }
          }
        }
      }
      policy-rematch;
      traceoptions {
        file filename <files number> <match regular-express>
        <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
      }
    }
    screen {
      ids-option screen-name{
        alarm-without-drop;
          icmp {
            flood {
              threshold number;
            }
            fragment;
            ip-sweep {
              threshold number;
            }
            large;
            ping-death;
          }
          ip {
            bad-option;
            block-frag;
            loose-source-route-option;
            record-route-option;
            security-option;
            source-route-option;
            spoofing;
            stream-option;
            strict-source-route-option;
            tear-drop;
            timestamp-option;
            unknown-protocol;
          }
          limit-session {
            destination-ip-based number;
            source-ip-based number;
          }
          tcp {
            fin-no-ack;
            land;
            port-scan {
              threshold number;
            }
```

```
            syn-ack-ack-proxy {
              threshold number;
            }
            syn-fin;
            syn-flood {
              alarm-thresholdnumber;
              attack-thresholdnumber;
              destination-threshold number;
              source-threshold number;
              timeout seconds;
            }
            syn-frag;
            tcp-no-flag;
            tcp-sweep {
              threshold number;
            }
            winnuke;
          }
          udp {
            flood {
              threshold number;
            }
            udp-sweep {
              threshold number;
            }
          }
        }
        traceoptions {
          file filename <files number> <match regular-expression>
          <size maximum-file-size> <world-readable | no-world-readable>;
          flag flag;
        }
      }
    }
    ssh-known-hosts {
      fetch-from-server fetch-from-server;
      host hostname {
        dsa-key base64-encoded-dsa-key;
        rsa-key base64-encoded-dsa-key;
        rsa1-key base64-encoded-dsa-key;
      }
      load-key-file key-file;
    }
    traceoptions {
      file filename {
        <files number>;
        <match regular-expression>;
        <size maximum-file-size>;
        <world-readable | no-world-readable>;
      }
      flag flag;
      no-remote-trace;
      rate-limit rate;
    }
    utm {
      custom-objects {
```


Copyright © 2011, Juniper Networks, Inc.

```
filename-extension {
   value [list];
   }
   mime-pattern {
   value [list];
   }
   custom-url-category {
   value [list];
   }
   protocol-command {
   value [list];
   }
   url-pattern {
   value [list];
   }
}
feature-profile {
anti-virus {
   type kaspersky-lab-engine;
      kaspersky-lab-engine {
      pattern-update {
         url;
            interval value;
         }
         profile profile-name {
         fallback-options {
            default (log-and-permit | block);
               corrupt-file (log-and-permit | block);
               password-file (log-and-permit | block);
               decompress-layer (log-and-permit | block);
               content-size (log-and-permit | block);
               engine-not-ready (log-and-permit | block);
               timeout (log-and-permit | block);
               out-of-resources (log-and-permit | block);
               too-many-requests (log-and-permit | block);
            }
            scan-options {
            intelligent-prescreening;
               scan-mode (scan-all | by--extension);
               content-size-limit value;
               timeout value;
               decompress-layer-limit value;
            }
            notification-options {
            virus-detection {
               type (message | protocol-only);
                  notify-mail-sender;
                  custom-message;
               }
               fallback-block {
               custom-message;
                  notify-mail-sender;
                  type;
               }
            }
            trickling {
```

```
            timeout value;
          }
        }
      }
      type juniper-express-engine;
      juniper-express-engine {
      pattern-update {
        url;
          interval value;
        }
        profile profile-name {
        fallback-options {
          default (log-and-permit | block);
            content-size (log-and-permit | block);
            engine-not-ready (log-and-permit | block);
            timeout (log-and-permit | block);
            out-of-resources (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
          scan-options {
          intelligent-prescreening;
            scan-mode (scan-all | by--extension);
            content-size-limit value;
            timeout value;
            decompress-layer-limit value;
          }
          notification-options {
          virus-detection {
            type (message | protocol-only);
              notify-mail-sender;
              custom-message;
            }
            fallback-block {
            custom-message;
              notify-mail-sender;
              type;
            }
          }
          trickling {
            timeout value;
          }
        }
        mime-whitelist {
        list listname {
          exception listname;
        }
        url-whitelist {
        listname;
        }
      }
    }
    web-filtering {
    surf-control-integrated {
      cache {
        timeout value;
        }
```

 Copyright © 2011, Juniper Networks, Inc.

```
        server {
        host host-name;
          port number;
        }
      profile profile-name{
        default (log-and-permit | block);
          custom-block-message value;
          fallback-settings {
          default (log-and-permit | block);
            server-connectivity (log-and-permit | block);
            timeout (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
          category customurl-list name {
          action (log-and-permit | block);
          }
        }
      websense-redirect {
      profile profile-name {
      server {
        host host-name;
          port number;
        }
        sockets value;
          timeout value;
          fallback-settings {
          default (log-and-permit | block);
            server-connectivity (log-and-permit | block);
            timeout (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
        }
      url-whitelist {
      listname;
      }
      url-blacklist {
      listname;
        }
      juniper-local {
          profile profile-name{
            custom-block-message value;
            default (block | log-and-permit | permit);
            fallback-settings {
              default (block | log-and-permit);
              timeout;
              too-many-requests (block | log-and-permit);
            }
            timeout
    }
    anti-spam {
    sbl {
      profile profile-name{
        sbl-default-server;
          spam-action (log-and-permit | block);
          custom-tag-string [***SPAM***];
        }
```

```
        address-whitelist{
        listname;
        }
      }
    }
    content-filtering {
    profile profile-name{
      block-command protocol-command-list;
        block-content-type (java-applet | exe | http-cookie);
        block-mime {
        list list-name {
          exception list-name;
          }
        }
      permit-command protocol-command-list;
      notification-options {
      type (message | protocol-only);
        custom-message [message];
      }
    }
    sophos-engine {
        pattern-update {
          email-notify {
            admin–email email address;
            custom-message message;
            custom-message-subject message;
          }
          interval <minutes>;
          no-autoupdate;
          url  <url>;
          }
        }
        profile <name> {
          fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resource (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
          }
          notification-options {
            fallback-block {
              administrator-email email address;
              allow-email;
              custom-message message;
              custom-message-subject subject;
              display-host;
              no-notify-mail-sender;
              notify-mail-sender;
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject subject;
              no-notify-mail-recipient;
```

 Copyright © 2011, Juniper Networks, Inc.

```
                notify-mail-recipient;
              }
              virus-detection {
                custom-message message;
                custom-message-subject subject;
                no-notify-mail-sender;
                notify-mail-sender;
                type (protocol-only | message );
              }
            }
            scan-options {
              content-size-limit value;
              no-uri-check;
              timeout minutes;
              uri-check;
            }
            trickling {
              timeout value;
            }
          }
          sxl-timeout seconds;
          sxl-retry value;
        }
}
utm-policy policy-name {
anti-virus {
  http-profile profile-name;
    ftp {
    upload-profile profile-name;
      download-profile profile-name;
    }
    smtp-profile profile-name;
    pop3-profile profile-name;
    imap-profile profile-name;
  }
  content-filtering {
  http-profile profile-name;
    ftp {
    upload-profile profile-name;
      download-profile profile-name;
    }
    smtp-profile profile-name;
    pop3-profile profile-name;
    imap-profile profile-name;
  }
  anti-spam {
  smtp-profile profile-name;
  }
  web-filtering {
  http-profile profile-name;
  }
  traffic-options {
  sessions-per-client {
    limit value;
      over-limit (log-and-permit | block);
    }
```

```
            }
          }
        }
      zones {
        functional-zone {
          management {
            host-inbound-traffic {
              protocols {
                protocol-name;
                protocol-name <except>;
              }
              system-services {
                service-name;
                service-name <except>;
              }
            }
            interfaces interface-name {
              host-inbound-traffic {
                protocols {
                  protocol-name;
                  protocol-name <except>;
                }
                system-services {
                  service-name;
                  service-name <except>;
                }
              }
            }
            screen screen-name;
          }
        }
        security-zone zone-name {
          address-book {
            address address-name (ip-prefix | dns-name dns-address-name |
              wildcard-address ipv4–address/wildcard-mask) ;
            address-set address-set-name {
              address address-name ;
            }
          }
          host-inbound-traffic {
            protocols {
              protocol-name;
              protocol-name <except>;
            }
            system-services {
              service-name;
              service-name <except>;
            }
          }
          interfaces interface-name {
            host-inbound-traffic {
              protocols {
                protocol-name;
                protocol-name <except>;
              }
              system-services {
```


Copyright © 2011, Juniper Networks, Inc.

```
                service-name;
                service-name <except>;
            }
        }
    }
    screen screen-name;
    tcp-rst;
  }
}
```

Related Documentation

- *Junos OS Security Configuration Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS System Basics Configuration Guide*

access-profile (Dynamic VPNs)

Syntax access-profile *profile-name*;

Hierarchy Level [edit security dynamic-vpn]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Specify the access profile to use for extended authentication for remote users trying to download the Access Manager.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

access-profile (IPsec VPNs)

Syntax access-profile *profile-name*;

Hierarchy Level [edit security ike gateway *gateway-name* xauth]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the access profile to use for extended authentication for remote users trying to access a Virtual Private Network (VPN) tunnel.

Options ***profile-name*** —Name of the access profile.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ack-number

Syntax

```
ack-number {
  match (equal | greater-than | less-than | not-equal);
  value acknowledgement-number ;
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify the ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***acknowledgement-number*** —Match the ACK number of the packet.

Range: 0 through 4,294,967,295

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

action

Syntax

```
action {
   (close-client | close-client-and-server | close-server |
   drop-connection | drop-packet | ignore-connection |
   class-of-service { forwarding-class forwarding-class-name; dscp-code-point value } |
   mark-diffserv  value  | no-action | recommended);
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the actions you want IDP to take when the monitored traffic matches the attack objects specified in the rules.

Options

- **close-client**—Closes the connection and sends an RST packet to the client but not to the server.
- **close-client-and-server**—Closes the connection and sends an RST packet to both the client and the server.
- **close-server**—Closes the connection and sends an RST packet to the server but not to the client.
- **drop-connection**—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.
- **drop-packet**—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
- **class-of-service**—Associates a class-of-service forwarding class as an action to the IDP policy; also sets the value of the DSCP code point. You can use the default forwarding class names or define new ones. Forwarding-class and dscp-code-point are optional, but one must be set.
- **ignore-connection**—Stops scanning traffic for the rest of the connection if an attack match is found. IDP disables the rulebase for the specific connection.
- **mark-diffserv** ***value*** —Assigns the indicated service-differentiation value to the packet in an attack, then passes them on normally.
- **no-action**—No action is taken. Use this action when you want to only generate logs for some traffic.
- **recommended**—All predefined attack objects have a default action associated with them. This is the action that Juniper Networks recommends when that attack is detected.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

action (Application-Level DDoS)

Syntax

```
action {
   [close-server | drop-connection | drop-packet | no-action]
}
```

Hierarchy Level
[edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then]

Release Information
Statement introduced in Release 10.0 of Junos OS.

Description
Specify the actions you want IDP to take when the monitored traffic matches the application-ddos objects specified in the application-level DDoS rule.

Options
- **close-server**—Closes the connection and sends an RST packet to the server but not to the client.
- **drop-connection**—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.
- **drop-packet**—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
- **no-action**—No action is taken. Use this action when you want to only generate logs for some traffic.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

action (web filtering)

Syntax action (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* category *customurl-list-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter an action to go with the customurl-list filter.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

active-policy

Syntax active-policy *policy-name* ;

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify which policy among the configured policies to activate.

Options *policy-name* —Name of the active policy.

NOTE: You need to make sure the active policy is enforced in the data plane.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

action-profile

Syntax

```
action-profile {
  event (jexec | lbt | mac-egress | mac-ingress | np-egress | np-ingress | pot)
    {
      count;
      packet-dump;
      packet-summary;
      trace;
    }
    module {
      flow {
        flag {
          all;
        }
      }
    }
    preserve-trace-order;
    record-pic-history;
```

Hierarchy Level [edit security datapath-debug]

Release Information Command introduced in Release 10.0 of Junos OS.

Description Configure the action profile options for data path debugging.

Options ***action-profile name*** — Name of the action profile.

event—Enable the events to trace the packet when the packet hit the events (jexec, lbt, mac-egress, mac-ingress, np-egress, np-ingress, pot)

- count—Number of times a packet hits the specified event.
- packet-dump—Capture the packet that hits the specified event.
- packet-summary—Print the source/destination IP address details with protocol number and IP length details along with trace message for the specified event.
- trace—Print the standard trace message when the packet hits the specified event.

module—Turn on the flow session related trace messages.

- flow—Trace flow session related messages.
- flag—Specify which flow message needs to be traced.
- all—Trace all possible flow trace messages.
- trace—Print the standard trace message when the packet hits the specified event.

preserve-trace-order—Preserve trace order.

record-pic-history—Record the PICs in which the packet has been processed.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address (ARP Proxy)

Syntax address *ip-address* to *ip-address* ;

Hierarchy Level [edit security nat proxy-arp interface *interface-name*],
[edit security nat source pool *pool-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a single address or an address range of ARP proxy.

Options **to**—Specify the upper limit of the address range.

ip-address —IP address of an ARP proxy.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address (Destination NAT)

Syntax address < *ip-address* > (to *ip-address* | port *port-number*);

Hierarchy Level [edit security nat destination pool *pool-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a single address or an address range of the destination NAT pool.

Options **to**—Specify the upper limit of the address range.

ip-address —IP address of a pool.

port ***port-number*** —Specify the port number.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address (IKE Gateway)

Syntax address [(*ip-address* | *hostname*)];

Hierarchy Level [edit security group-vpn member ike gateway *gateway-name*]
[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description Specify the IPv4 or IPv6 address or the hostname of the primary Internet Key Exchange (IKE) gateway and up to four backup gateways.

Options ***ip-address* | *hostname*** —IPv4 or IPv6 address or hostname of an IKE gateway.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

address (Zone Address Book)

Syntax

address *address-name* *(ip-prefix* | dns-name *dns-address-name* | wildcard-address *ipv4–address/wildcard-mask)* ;

Hierarchy Level

[edit security zones security-zone *zone-name* address-book]

Release Information

Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description

Add an entry containing an IP address or domain name system (DNS) hostname or wildcard address to the address book for a security zone. A zone's address book contains entries for addressable entities in policy definitions.

Options

address-name— Name of the address entry.

ip-prefix— IP address with prefix. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and DNS names.

dns-name ***dns-address-name*** —DNS address name.

wildcard-address ***ipv4-address/wildcard-mask*** —IPv4 wildcard address in the form A.B.C.D/wildcard-mask.

NOTE: IPv6 wildcard address configuration is not supported in this release.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

address-book

Syntax

```
address-book {
  address address-name (ip-prefix | dns-name dns-address-name | wildcard-address
    ipv4–address/wildcard-mask);
  address-set address-set-name {
    address address-name ;
  }
}
```

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description Define entries in the address book of a security zone. An address book is a list containing all addresses and address groups, domain name system (DNS) names, and wildcard addresses defined for a security zone. You use address-book entries to identify addressable entities in policy definitions. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, and wildcard addresses.

NOTE: IPv6 wildcard address configuration is not supported in this release.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address-blacklist

Syntax

```
address-blacklist{
listname;
}
```

Hierarchy Level [edit security utm feature-profile anti-spam]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter an address-blacklist (or whitelist) custom-object for local list spam filtering.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

address-mapping

Syntax address-mapping;

Hierarchy Level [edit security nat source rule-set *ruleset* rule *rule* then source-nat (pool | interface) persistent-nat]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Allows requests from a specific internal IP address to be mapped to the same reflexive IP address (the public IP address created by the NAT device closest to the STUN server); internal and external ports can be any ports. An external host using any port can send a packet to the internal host by sending the packet to the reflexive IP address (with a configured incoming policy that allows external to internal traffic). If this option is not configured, the persistent NAT binding is for specific internal and reflexive transport addresses.

You can only specify this option when the persistent NAT type is **any-remote-host** and the source NAT rule action is one of the following:

- Source NAT pool with IP address shifting
- Source NAT pool with no port translation and no overflow pool

Required Privilege Level **security**—To view this statement in the configuration.
security-control—To add this statement to the configuration

Related Documentation
- *Junos OS Security Configuration Guide*

address-persistent

Syntax address-persistent;

Hierarchy Level [edit security nat source]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Enable the device to assign the same IP address from a source pool to a host for multiple concurrent sessions that require the same source IP address for each session.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address-set

Syntax

```
address-set address-set-name {
  address address-name ;
}
```

Hierarchy Level [edit security zones security-zone *zone-name* address-book]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Identify a collection of addresses, as defined with the **address (Zone Address Book)** statement.

Options ***address-set-name*** —Name of the address set.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

address-whitelist

Syntax

```
address-whitelist{
listname;
}
```

Hierarchy Level [edit security utm feature-profile anti-spam]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter an address-whitelist (or blacklist) custom-object for local list spam filtering.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

admin-email

Syntax admin-email *email address*;

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure the device to notify a specified administrator when patterns are updated. This is an email notification with a custom message and a custom subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

administrator

Syntax
```
administrator {
  e-mail-address e-mail-address ;
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify an administrator e-mail address to which the certificate request is sent.

Options **e-mail-address** ***e-mail-address*** —E-mail address where the certificate request is sent. By default, there is no preset e-mail address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

administrator-email (fallback-block)

Syntax administrator-email *email address*;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options fallback-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the administrator e-mail address that will be notified when a fallback-block occurs in Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

administrator-email (virus-detection)

Syntax administrator-email *email address*;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options virus-detection]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the administrator e-mail address that will be notified when a virus is detected by Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

aging

Syntax

```
aging {
   early-ageout seconds ;
   high-watermark percent ;
   low-watermark percent ;
}
```

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Direct the device to begin aggressively aging out sessions when the percentage of entries in the session table exceeds the high-watermark setting and then stops when the percentage of sessions falls below the low-watermark setting.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

alarm-threshold

Syntax alarm-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the number of half-complete proxy connections per second at which the device makes entries in the event alarm log.

Options *number* —Threshold value.

Range: 1 through 100,000 per second

Default: 1024 per second

NOTE: For SRX Series devices the applicable range is 1 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

alarm-without-drop

Syntax alarm-without-drop;

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Direct the device to generate an alarm when detecting an attack but not block the attack. Use this statement to allow an attack to enter a segment of your network that you have previously prepared to receive it (for example, a honeynet, which is a decoy network with extensive monitoring capabilities).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

alert

Syntax alert;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification log-attacks]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set an alert flag in the Alert column of the Log Viewer for the matching log record.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

alg

Syntax

```
alg {
  dns {
    disable;
    maximum-message-length number;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  ftp {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  h323 {
    application-screen {
      message-flood {
        gatekeeper threshold rate ;
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    endpoint-registration-timeout seconds ;
    media-source-port-any;
    traceoptions {
      flag {
        all <detail | extensive | terse>;
        cc <detail | extensive | terse>;
        h225-asn1 <detail | extensive | terse>;
        h245 <detail | extensive | terse>;
        h245-asn1 <detail | extensive | terse>;
        q931 <detail | extensive | terse>;
        ras <detail | extensive | terse>;
        ras-asn1 <detail | extensive | terse>;
      }
    }
  }
  ike-esp-nat {
    enable;
    state-timeout timeout-in-seconds;
    esp-gate-timeout timeout-in-seconds;
    esp-session-timeout timeout-in-seconds;
  }
  mgcp {
    application-screen {
```

```
        connection-flood threshold rate ;
        message-flood threshold rate ;
        unknown-message {
          permit-nat-applied;
          permit-routed;
        }
      }
      disable;
      inactive-media-timeout seconds ;
      maximum-call-duration minutes ;
      traceoptions {
        flag {
          all <extensive>;
          call <extensive>;
          cc <extensive>;
          decode <extensive>;
          error <extensive>;
          nat <extensive>;
          packet <extensive>;
          rm <extensive>;
        }
      }
      transaction-timeout seconds ;
    }
    msrpc {
      disable;
      traceoptions {
        flag {
          all <extensive>;
        }
      }
    }
    pptp {
      disable;
      traceoptions {
        flag {
          all <extensive>;
        }
      }
    }
    real {
      disable;
      traceoptions {
        flag {
          all <extensive>;
        }
      }
    }
    rsh {
      disable;
      traceoptions {
        flag {
          all <extensive>;
        }
      }
    }
```


Copyright © 2011, Juniper Networks, Inc.

```
rtsp {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
sccp {
   application-screen {
      call-flood threshold rate ;
      unknown-message {
         permit-nat-applied;
         permit-routed;
      }
   }
   disable;
   inactive-media-timeout seconds ;
   traceoptions {
      flag {
         all <extensive>;
         call <extensive>;
         cc <extensive>;
         cli <extensive>;
         decode <extensive>;
         error <extensive>;
         init <extensive>;
         nat <extensive>;
         rm <extensive>;
      }
   }
}
sip {
   application-screen {
      protect {
         deny {
            all | destination-ip address ;
            timeout seconds ;
         }
      }
      unknown-message {
         permit-nat-applied;
         permit-routed;
      }
   }
   c-timeout minutes ;
   disable;
   disable-call-id-hiding;
   inactive-media-timeout seconds ;
   maximum-call-duration minutes ;
   retain-hold-resource;
   t1-interval milliseconds ;
   t4-interval seconds ;
   traceoptions {
      flag {
         all <detail | extensive | terse>;
```

```
            call <detail | extensive | terse>;
            cc <detail | extensive | terse>;
            nat <detail | extensive | terse>;
            parser <detail | extensive | terse>;
            rm <detail | extensive | terse>;
          }
        }
      }
      sql {
        disable;
        traceoptions {
          flag {
            all <extensive>;
          }
        }
      }
      sunrpc {
        disable;
        traceoptions {
          flag {
            all <extensive>;
          }
        }
      }
      talk {
        disable;
        traceoptions {
          flag {
            all <extensive>;
          }
        }
      }
      tftp {
        disable;
        traceoptions {
          flag {
            all <extensive>;
          }
        }
      }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure an Application Layer Gateway (ALG) on the device. An ALG runs as a service and can be associated in policies with specified types of traffic. ALGs are enabled by default.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

Related Documentation
- *Junos OS Security Configuration Guide*

algorithm

Syntax
algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);

Hierarchy Level
[edit security ipsec vpn *vpn-name* manual encryption]

Release Information
Statement modified in Release 8.5 of Junos OS.

Description
Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration. (This statement is not supported on dynamic VPN implementations.)

Options
3des-cbc—3DES-CBC encryption algorithm.

aes-128-cbc—AES-CBC 128-bit encryption algorithm.

aes-192-cbc—AES-CBC 192-bit encryption algorithm.

aes-256-cbc—AES-CBC 256-bit encryption algorithm.

des-cbc—DES-CBC encryption algorithm.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

all-tcp

Syntax
```
all-tcp {
  mss value ;
}
```

Hierarchy Level
[edit security flow tcp-mss]

Release Information
Statement introduced in Release 8.5 of Junos OS.

Description
Set the TCP maximum segment size (MSS) value for all TCP packets for network traffic.

Options
mss *value* —TCP MSS value.
Range: 64 through 65,535 bytes

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

allow-dns-reply

Syntax allow-dns-reply;

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Allow an incoming Domain Name Service (DNS) reply packet without a matched request. By default, if an incoming UDP first-packet has dst-port 53, the device checks the DNS message packet header to verify that the query bit (QR) is 0, which denotes a query message. If the QR bit is 1, which denotes a response message, the device drops the packet, does not create a session, and increments the illegal packet flow counter for the interface. Using the **allow-dns-reply** statement directs the device to skip the check.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

allow-email (fallback-block)

Syntax allow-email;

Hierarchy Level [edit security utm feature-profile anti-virus profile notification-options fallback-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Enable e-mail notification to notify a specified administrator when a fallback-block occurs.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

allow-email (virus-detect)

Syntax allow–email;

Hierarchy Level [edit security utm feature-profile anti-virus profile notification-options virus-detect]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Enable e-mail notification to notify a specified administrator when a virus is detected.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

allow-icmp-without-flow

Syntax (allow-icmp-without-flow | no-allow-icmp-without-flow);

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Allow an ICMP packet without matched request. By default the ICMP flow is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

always-send

Syntax always-send;

Hierarchy Level [edit security ike gateway *gateway-name* dead-peer-detection]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Instructs the device to send dead peer detection (DPD) requests regardless of whether there is outgoing IPsec traffic to the peer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

analysis no-reports

Syntax analysis no-reports;

Hierarchy Level [edit security]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description By default, logging information is automatically reported with the J-Web reporting feature. Specify the **analysis no-reports** option of the **edit security** statement to turn off reporting.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

anomaly

Syntax

```
anomaly {
   direction (any | client-to-server | server-to-client);
   service  service-name ;
   shellcode (all | intel | no-shellcode | sparc);
   test  test-condition ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

antispam (feature-profile)

Syntax

```
anti-spam {
sbl {
   profile profile-name{
      sbl-default-server;
         spam-action (log-and-permit | block);
         custom-tag-string [***SPAM***];
      }
      address-whitelist{
      listname;
      }
      address-blacklist{
      listname;
      }
   }
}
```

Hierarchy Level [edit security utm feature-profile]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure UTM antispam features.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

antispam (utm-policy)

Syntax

```
anti-spam {
smtp-profile profile-name;
}
```

Hierarchy Level [edit security utm utm-policy *policy-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

antivirus (feature-profile)

Syntax

```
anti-virus {
type kaspersky-lab-engine;
  kaspersky-lab-engine {
  pattern-update {
    url;
      interval value;
    }
    profile profile-name {
    fallback-options {
      default (log-and-permit | block);
        corrupt-file (log-and-permit | block);
        password-file (log-and-permit | block);
        decompress-layer (log-and-permit | block);
        content-size (log-and-permit | block);
        engine-not-ready (log-and-permit | block);
        timeout (log-and-permit | block);
        out-of-resources (log-and-permit | block);
        too-many-requests (log-and-permit | block);
      }
      scan-options {
      intelligent-prescreening;
        scan-mode (scan-all | by--extension);
        content-size-limit value;
        timeout value;
        decompress-layer-limit value;
      }
      notification-options {
      virus-detection {
        type (message | protocol-only);
          notify-mail-sender;
          custom-message;
        }
        fallback-block {
        custom-message;
          notify-mail-sender;
          type;
        }
      }
      trickling {
        timeout value;
      }
    }
  }
  type juniper-express-engine;
  juniper-express-engine {
  pattern-update {
    url;
      interval value;
    }
    profile profile-name {
    fallback-options {
      default (log-and-permit | block);
```

```
            content-size (log-and-permit | block);
            engine-not-ready (log-and-permit | block);
            timeout (log-and-permit | block);
            out-of-resources (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
          scan-options {
          intelligent-prescreening;
            scan-mode (scan-all | by--extension);
            content-size-limit value;
            timeout value;
            decompress-layer-limit value;
          }
          notification-options {
          virus-detection {
            type (message | protocol-only);
              notify-mail-sender;
              custom-message;
            }
            fallback-block {
            custom-message;
              notify-mail-sender;
              type;
            }
          }
          trickling {
            timeout value;
          }
        }
        mime-whitelist {
        list listname {
          exception listname;
        }
        url-whitelist {
        listname;
        }
      }
    }
```

Hierarchy Level [edit security utm feature-profile]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure UTM antivirus full and express features.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

antivirus (utm-policy)

Syntax

```
anti-virus {
http-profile profile-name;
   ftp {
   upload-profile profile-name;
      download-profile profile-name;
   }
   smtp-profile profile-name;
   pop3-profile profile-name;
   imap-profile profile-name;
}
```

Hierarchy Level [edit security utm utm-policy *policy-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus protocols and attach this policy to a security profile to implement it.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

apn (gtp)

Syntax

```
apn pattern-string {
  mcc-mnc <mcc-mnc-number> {
    action <drop | pass | selection <ms | net | vrf> {
      }
    }
```

Hierarchy Level

[edit security gprs gtp profile *profile name* apn]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Allow or deny access to specific Access Point Names (APNs)

- *pattern-string*—Set an APN suffix such as “juniper.net.mcc123.mnc456.gprs”.
- **drop**—Specify to deny GTP packets from all Selection Modes for this APN.
- **pass**—Specify to permit GTP packets from all Selection Modes for this APN.
- **selection**—Specify one of the following Selection Modes for the APN:
  - **ms** The APN is provided by a mobile station (MS) and the user-subscription is not verified.
  - **net** The APN is provided by a network and the user-subscription is not verified.
  - **vrf** The APN is provided by a network or an MS and the user-subscription is verified.

NOTE: Because APN filtering is based on a perfect match, using the wildcard * when setting an APN suffix can prevent the inadvertent exclusion of APNs you would otherwise authorize. The security device automatically permits all other APNs that do not match. The wildcard * can only be used as the first character in the APN string.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

application (Application-Level DDoS)

Syntax application [any | default];

Hierarchy Level [edit security idp idp-policy *idp-policy-name* rulebase-ddos rule *rule-name* match]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the application or application-set name to match.

Options ***any***—Match all ports to the only application implied in the attack objects.

default—Match default and automatically detected ports to the applications implied in the attack object.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application (Protocol Binding Custom Attack)

Syntax application ***application-name*** ;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the attack for a specified application.

Options ***application-name*** —Name of the application.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application (Security Policies)

Syntax application [*application-name-or-set*];

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

Options *application-name-or-set* —Name of the application or application set used as match criteria.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

application-firewall

Syntax

```
application-firewall {
  rule-sets {
    rule-set-name {
      rule rule-name {
        match {
          dynamic-application [ dynamic-application-names];
        }
        then {
          permit | deny;
        }
      }
      default-rule {
        permit | deny;
      }
    }
  }
  traceoptions {
    file filename {
      <files number>;
      <match regular-expression>;
      <size maximum-file-size >;
      <world-readable | no-world-readable>;
    }
    flag {
      all;
      compilation;
      configuration;
      ipc;
      lookup;
    }
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure application firewall rule sets with rules defining match criteria and the action to be performed.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

application-identification

Syntax

```
application-identification {
   application-system-cache;
   application-system-cache-timeout value;
   disable;
   max-packet-memory value;
   max-sessions value;
   max-tcp-session-packet-memory value;
   max-udp-session-packet-memory value;
   nested-application-system-cache;
   nested-application;
}
```

Hierarchy Level

[edit security idp sensor-configuration]

Release Information

Statement introduced in Release 9.2 of Junos OS.

Description

Enable to identify the TCP/UDP application session running on nonstandard ports to match the application properties of transiting network traffic.

Options

disable—Disable the TCP/UDP application identification of nonstandard ports' matching properties.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

application-screen (H323)

Syntax

```
application-screen {
  message-flood {
    gatekeeper threshold rate ;
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

Hierarchy Level [edit security alg h323]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the security screens for the H.323 protocol Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-screen (MGCP)

Syntax

```
application-screen {
  connection-flood threshold rate ;
  message-flood threshold rate ;
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the security screens for the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-screen (SCCP)

Syntax

```
application-screen {
   call-flood threshold rate ;
   unknown-message {
      permit-nat-applied;
      permit-routed;
   }
}
```

Hierarchy Level [edit security alg sccp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the security screens for the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

application-screen (SIP)

Syntax

```
application-screen {
  protect {
    deny {
      all | destination-ip address ;
      timeout seconds ;
    }
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the security screens for the Session Initiation Protocol (SIP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

application-services (Application Firewall)

Syntax

```
application-services {
  application-firewall {
    rule-set rule-set-name;
  }
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information

Statement modified in Release 11.1 of Junos OS.

Description

Enable application firewall within the security policy. This statement is required when configuring the SRX Series devices to enable additional security control against dynamic applications.

Options

The remaining statements are explained separately.

Usage Guidelines

For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

application-services (Priority)

Syntax

```
application-services {
  maximize-alg-sessions;
  maximize-cp-sessions;
  maximize-idp-sessions {
    inline-tap;
    weight {
      equal;
      firewall;
      idp;
    }
  }
}
```

Hierarchy Level [edit security forwarding-process]

Release Information Statement introduced in Release 9.6 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

Description You can configure the device to switch from an integrated firewall mode to maximize IDP mode to increase the capacity of IDP processing with the **maximize-idp-sessions** option. When you maximize IDP, you are decoupling IDP processes from firewall processes, allowing the device to support the same number of firewall and IDP sessions.

With the **maximize-cp-sessions** option you can increase the maximum number of central point sessions from 12.5 million sessions to 14 million sessions on a fully loaded SRX5800 device. Note that this option is supported only on SRX5800 devices. Using this optimization technique precludes other optimization methods, disables advanced GTP processing, and reduces routing capacity to 100K prefixes.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

application-services (Unified Access Control)

Syntax application-services (uac-policy);

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement modified in Release 9.4 of Junos OS.

Description Enable Unified Access Control (UAC) for the security policy. This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-services (WXC Integrated Services Module)

Syntax application-services (redirect-wx | reverse-redirect-wx);

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define the acceleration zone security policy for WX redirection of packets to the WXC Integrated Service Module (ISM 200) for WAN acceleration. During the redirection process, the direction of the WX packet and its type determine further processing of the packet.

Options **redirect-wx**—Specify the WX redirection needed for the packets that arrive from the LAN.

reverse-redirect-wx—Specify the WX redirection needed for the reverse flow of the packets that arrive from the WAN.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

application-system-cache

Syntax application-system-cache;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description When a session is created, specify an application ID to match the application properties of transiting network traffic. The application port mappings are saved in the application system cache.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-system-cache-timeout

Syntax application-system-cache-timeout *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]
[edit services application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS. Support for application identification in the services hierarchy added in 10.2.

Description Specify the timeout value in seconds for the application system cache entries. Note the cache is not cleared when IDP policy is loaded. Users need to manually clear or wait for the cache entries to expire.

Options *value* —Timeout value for the application system cache entries.

Range: 0 through 1,000,000 seconds

Default: 3600 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

application-tracking

Syntax

```
application-tracking {
   first-update;
   first-update-interval number;
   session-update-interval number;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description AppTrack, an application tracking tool, is a form of statistical profiling. Enabling this feature for a zone logs flow statistics (the byte count, packet count, and start and end times for a session) at session end. You can modify the logging time and log frequency with command options. Periodically, a network management tool, such as STRM, collects the logged statistics sent by each network device for bandwidth usage analysis of the network.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

association-timeout

Syntax association-timeout *time in minutes*;

Hierarchy Level [edit security gprs sctp profile *name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Set the association timeout for Stream Control Transmission Protocol (SCTP).

Options **minutes**—Number of minutes of association time that elapse before the session is terminated.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

attack-threshold

Syntax attack-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the number of SYN packets per second required to trigger the SYN proxy response.

Options *number* —Number of SYN packets per second required to trigger the SYN proxy response.

Range: 1 through 100,000 per second

Default: 200 per second

NOTE: For SRX Series devices, the applicable range is 1 through 1.000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

attacks (Exempt Rulebase)

Syntax

```
attacks {
  custom-attacks [attack-name];
  predefined-attack-groups [attack-name];
  predefined-attacks [attack-name];
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the attacks that you do not want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

attacks (IPS Rulebase)

Syntax

```
attacks {
  custom-attacks [attack-name];
  predefined-attack-groups [attack-name];
  predefined-attacks [attack-name];
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the attacks you want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

attack-type (Anomaly)

Syntax

```
attack-type {
  anomaly {
    direction (any | client-to-server | server-to-client);
    service service-name ;
    shellcode (all | intel | no-shellcode | sparc);
    test test-condition ;
  }
}
```

Hierarchy Level [edit security idp custom-attack *attack-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the type of attack.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

attack-type (Chain)

Syntax

```
attack-type {
  chain {
    expression boolean-expression ;
    member member-name {
      attack-type {
        (anomaly | signature);
      }
    }
    order;
    protocol-binding {
      application application-name ;
      icmp;
      ip {
        protocol-number transport-layer-protocol-number ;
      }
      rpc {
        program-number rpc-program-number ;
      }
      tcp {
        minimum-port port-number maximum-port port-number ;
      }
      udp {
        minimum-port port-number maximum-port port-number ;
      }
    }
    reset;
    scope (session | transaction);
  }
```

Hierarchy Level

[edit security idp custom-attack *attack-name*]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify the type of attack.

NOTE: In a chain attack, you can configure multiple member attacks.

In an attack, under protocol binding TCP/UDP, you can specify multiple ranges of ports.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

attack-type (Signature)

Syntax

```
attack-type {
  signature {
    context context-name ;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern ;
    protocol {
      icmp {
        code {
          match (equal | greater-than | less-than | not-equal);
          value code-value ;
        }
        data-length {
          match (equal | greater-than | less-than | not-equal);
          value data-length ;
        }
        identification {
          match (equal | greater-than | less-than | not-equal);
          value identification-value ;
        }
        sequence-number {
          match (equal | greater-than | less-than | not-equal);
          value sequence-number ;
        }
        type {
          match (equal | greater-than | less-than | not-equal);
          value type-value ;
        }
      }
      ip {
        destination {
          match (equal | greater-than | less-than | not-equal);
          value hostname ;
        }
        identification {
          match (equal | greater-than | less-than | not-equal);
          value identification-value ;
        }
        ip-flags {
          (df | no-df);
          (mf | no-mf);
          (rb | no-rb);
        }
        protocol {
          match (equal | greater-than | less-than | not-equal);
          value transport-layer-protocol-id ;
        }
        source {
          match (equal | greater-than | less-than | not-equal);
          value hostname ;
        }
        tos {
```


Copyright © 2011, Juniper Networks, Inc.

```
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal ;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram ;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live ;
      }
    }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number ;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length ;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port ;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length ;
      }
      mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size ;
      }
      option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option ;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number ;
      }
      source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port ;
      }
      tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
      }
      urgent-pointer {
```

```
            match (equal | greater-than | less-than | not-equal);
            value urgent-pointer ;
          }
          window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor ;
          }
          window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size ;
          }
        }
        udp {
          data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length ;
          }
          destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port ;
          }
          source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port ;
          }
        }
      }
      protocol-binding {
        application application-name ;
        icmp;
        ip {
          protocol-number transport-layer-protocol-number ;
        }
        rpc {
          program-number rpc-program-number ;
        }
        tcp {
          minimum-port port-number maximum-port port-number ;
        }
        udp {
          minimum-port port-number maximum-port port-number ;
        }
      }
      regexp regular-expression ;
      shellcode (all | intel | no-shellcode | sparc);
    }
```

Hierarchy Level [edit security idp custom-attack *attack-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the type of attack.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

Related Documentation

- *Junos OS Security Configuration Guide*

authentication

Syntax

```
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key );
}
```

Hierarchy Level

[edit security ipsec vpn *vpn-name* manual]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Configure IP Security (IPsec) authentication parameters for a manual security association (SA). (This statement is not supported on dynamic VPN implementations.)

Options

algorithm—Hash algorithm that authenticates packet data. It can be one of the following:

- **hmac-md5-96**—Produces a 128-bit digest.

  hmac-sha1-96—Produces a 160-bit digest

key—Type of authentication key. It can be one of the following:

- **ascii-text *key***—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
- **hexadecimal *key***—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

authentication-algorithm

Syntax authentication-algorithm (md5 | sha1 | sha-256);

Hierarchy Level [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Configure the Internet Key Exchange (IKE) authentication algorithm.

Options **authentication-algorithm**—Hash algorithm that authenticates packet data. It can be one of three algorithms:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.
- **sha-256**—Produces a 256-bit digest.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

authentication-method

Syntax authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);

Hierarchy Level [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify the method the device uses to authenticate the source of Internet Key Exchange (IKE) messages. The **pre-shared-keys** option refers to a preshared key, which is a key for encryption and decryption that both participants must have before beginning tunnel negotiations. The **rsa-signatures** and **dsa-signatures** options refer to two kinds of digital signatures, which are certificates that confirm the identity of the certificate holder. (The default method is a preshared key.) (The **rsa-signatures** and **dsa-signatures** options are not supported on dynamic VPN implementations.)

Options **dsa-signatures**—Specify that the Digital Signature Algorithm (DSA) is used.

pre-shared-keys—Specify that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. This is the default method.

rsa-signatures—Specify that a public key algorithm, which supports encryption and digital signatures, is used.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

auto-re-enrollment

Syntax

```
auto-re-enrollment {
  certificate-id certificate-id-name {
    ca-profile-name ca-profile-name ;
    challenge-password password ;
    re-enroll-trigger-time-percentage percentage ;
    re-generate-keypair;
  }
}
```

Hierarchy Level [edit security pki]

Release Information Statement modified in Release 9.0 of Junos OS.

Description Configure the automatic reenrollment of a certificate authority (CA) certificate.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

automatic

Syntax

```
automatic {
  enable;
  interval hours ;
  start-time start-time ;
}
```

Hierarchy Level [edit security idp security-package]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable the device to automatically download the updated signature database from the specified URL.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

bind-interface

Syntax bind-interface *interface-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure the tunnel interface to which the route-based virtual private network (VPN) is bound.

Options *interface-name* —Tunnel interface.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

block-command

Syntax block-command *protocol-command-list*;

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Apply protocol block command custom-objects to the content-filtering profile

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

block-content-type

Syntax block-content-type (java-applet | exe | http-cookie);

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Apply blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

Options
- activex
- exe
- java-applet
- http-cookie
- zip

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

block-mime

Syntax

```
block-mime {
list list-name {
   exception list-name;
   }
}
```

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

bridge

Syntax

```
bridge {
  block-non-ip-all;
  bypass-non-ip-unicast;
  no-packet-flooding {
    no-trace-route;
  }
}
```

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Changes default Layer 2 forwarding behavior.

Options

block-non-ip-all—Block all Layer 2 non-IP and non-ARP traffic, including multicast and broadcast traffic.

no-packet-flooding—Stop IP flooding and send ARP or ICMP requests to discover the destination MAC address for a unicast packet.

no-trace-route—Do not send ICMP requests to discover the destination MAC address for a unicast packet. Only ARP requests are sent. This option only allows the device to discover the destination MAC address for a unicast packet if the destination IP address is in the same subnetwork as the ingress IP address.

bypass-non-ip-unicast—Allow all Layer 2 non-IP traffic to pass through the device.

NOTE: The **block-non-ip-all** and **bypass-non-ip-unicast** options cannot be configured at the same time.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

c-timeout

Syntax c-timeout *minutes* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the timeout interval for Session Initiation Protocol (SIP) transactions in minutes.

Options ***minutes*** —Timeout interval.
Range: 3 through 10 minutes
Default: 3 minutes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ca-identity

Syntax ca-identity *ca-identity* ;

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement modified in Release 11.1 of Junos OS.

Description Specify the certificate authority (CA) identity to use in requesting digital certificates.

Options ***ca-identity*** —Name of CA identity. This name is typically the domain name of the CA.

routing-instance-name —Name of routing instance. The routing instance name is chosen from the list of configured routing instances.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ca-profile

Syntax

```
ca-profile ca-profile-name {
  administrator {
    e-mail-address e-mail-address ;
  }
  ca-identity ca-identity ;
  routing-instance routing-instance-name ;
  enrollment {
    retry number;
    retry-interval seconds;
    url url-name;
  }
  revocation-check {
    crl {
      disable {
        on-download-failure;
      }
      refresh-interval hours ;
      url url-name ;
    }
    disable;
  }
}
```

Hierarchy Level [edit security pki]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure certificate authority (CA) profile.

Options *ca-profile-name* —Name of a trusted CA.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ca-profile-name

Syntax ca-profile-name *ca-profile-name* ;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id *certificate-id-name*]

Release Information Statement modified in Release 9.0 of Junos OS.

Description Specify the name of the certificate authority (CA) profile.

Options *ca-profile-name* —Name of the specific CA profile.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

cache

Syntax
```
cache {
timeout value;
}
```

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Set the cache timeout parameters for surf-control-integrated Web filtering (24 hours is the default and the maximum allowed life span for cached items).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

cache-size

Syntax cache-size *size*;

Hierarchy Level [edit security idp sensor-configuration log]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the size in bytes for each user's log cache.

Options **size**—Cache size.
Range: 1 through 65,535 bytes
Default: 12800 bytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

call-flood

Syntax call-flood threshold *rate* ;

Hierarchy Level [edit security alg sccp application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the number of calls per second allowed to Skinny Client Control Protocol (SCCP) client. Calls exceeding the threshold are dropped by the SCCP Application Layer Gateway (ALG).

Options **threshold** *rate* —Number of calls per second per client.
Range: 2 through 1000
Default: 20

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

category

Syntax

```
category {
  values [list-of-values];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name*filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a category filter to add attack objects based on the category.

Options **values**—Name of the category filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

category (Security Logging)

Syntax category (all | content-security)

Hierarchy Level [edit security log stream *stream-name* format (syslog | sd-syslog | welf)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

category (web filtering)

Syntax

```
category customurl-list name {
action (log-and-permit | block);
}
```

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile profile-name]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Select a custom URL category list you created (custom objects) for filtering against.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

certificate

Syntax

```
certificate {
  local-certificate certificate-id ;
  peer-certificate-type (pkcs7 | x509-signature);
  trusted-ca ( ca-index | use-all);
}
```

Hierarchy Level
[edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify usage of a digital certificate to authenticate the virtual private network (VPN) initiator and recipient. (This statement is not supported on dynamic VPN implementations.)

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

certificate-id

Syntax

```
certificate-id certificate-id-name {
   ca-profile-name ca-profile-name ;
   challenge-password password ;
   re-enroll-trigger-time-percentage percentage ;
   re-generate-keypair;
}
```

Hierarchy Level [edit security pki auto-re-enrollment]

Release Information Statement modified in Release 9.0 of Junos OS.

Description Specify the certificate authority (CA) certificate to use for automatic reenrollment.

Options ***certificate-id-name*** —Identifier of the certificate that needs automatic reenrollment.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

chain

Syntax

```
chain {
  expression boolean-expression ;
  member member-name {
    attack-type {
      (anomaly | signature);
    }
  }
  order;
  protocol-binding {
    application application-name ;
    icmp;
    ip {
      protocol-number transport-layer-protocol-number ;
    }
    rpc {
      program-number rpc-program-number ;
    }
    tcp {
      minimum-port port-number maximum-port port-number ;
    }
    udp {
      minimum-port port-number maximum-port port-number ;
    }
  }
  reset;
  scope (session | transaction);
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Chain attack object combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the chain attack object.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

challenge-password

Syntax challenge-password *password* ;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id *certificate-id-name*]

Release Information Statement modified in Release 9.0 of Junos OS.

Description Specify the password used by the certificate authority (CA) for enrollment and revocation. If the CA does not provide the challenge password, choose your own password.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

clear-threshold

Syntax clear-threshold *clear-threshold* ;

Hierarchy Level [edit security nat source pool-utilization-alarm]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the lower threshold at which an SNMP trap is triggered when pool utilization for a source pool without Port Address Translation (PAT) falls below the threshold.

Options *clear-threshold* —Threshold at which an SNMP trap is triggered.
Range: 40 through 100

Required Privilege Level security-To view this statement in the configuration.
security-control-To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

clients

Syntax

```
clients {
  configuration-name {
    remote-protected-resources {
      ip-address/mask;
    }
    remote-exceptions {
      ip-address/mask;
    }
    ipsec-vpn configuration-name;
    user {
      username;
    }
  }
}
```

Hierarchy Level [edit security dynamic-vpn]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to create a client configuration for the dynamic VPN feature. Within the configuration, specify a name for the configuration, reference a standard VPN configuration to use for IPsec negotiations, specify which resources to protect, define any exceptions, and list the users to which the dynamic VPN configuration applies.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

co-location

Syntax co-location;

Hierarchy Level [edit security group-vpn]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specifies that the group server and group member functions coexist in the same device. The group server and group member must have different IP addresses so that packets can be delivered properly. In colocation mode, there can only be one IP address assigned to the server and one IP address assigned to the member across groups.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

code

Syntax

```
code {
  match (equal | greater-than | less-than | not-equal);
  value code-value ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the secondary code that identifies the function of the request/reply within a given type.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***code-value*** —Match a decimal value.

Range: 0 through 255

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

connection-flood

Syntax connection-flood threshold *rate* ;

Hierarchy Level [edit security alg mgcp application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

Options

threshold ***rate*** —Number of connection requests per second allowed per MG.

Range: 2 through 10000

Default: 200

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

connection-rate-threshold

Syntax connection-rate–threshold *number*;

Hierarchy Level [edit security idp application-ddos *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the connections-per-second threshold at which to start monitoring the application context values for application-level DDoS protection.

Options **threshold *number***—connection rate requests per second.

Range:

- SRX3400/3600– 1 to 200,000
- SRX5600/5800–1 to 400,000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

connections-limit

Syntax connections-limit *number* ;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the number of concurrent connections that the group profile supports. When the maximum number of connections is reached, no more dynamic virtual private network (VPN) endpoints dialup users attempting to access an IPsec VPN are allowed to begin Internet Key Exchange (IKE) negotiations.

Options ***number*** —Maximum number of concurrent connections allowed.

Range: 1 through 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

container

Syntax container *container-string*;

Hierarchy Level [edit security group-vpn server ike gateway *gateway-name* dynamic distinguished-name]
[edit security ike gateway *gateway-name* dynamic distinguished-name]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description Specify that the value in the identity fields of a dynamic virtual private network (VPN) endpoint user's distinguished name exactly match the values in the group IKE user's distinguished name. The order of the identity fields in the fields of the distinguished name strings must be identical when matching. (This statement is not supported on dynamic VPN implementations.)

Options ***container-string***—Distinguished name identity value to be matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

content-filtering (feature-profile)

Syntax

```
content-filtering {
profile profile-name{
  block-command protocol-command-list;
    block-content-type (java-applet | exe | http-cookie);
    block-mime {
    list list-name {
      exception list-name;
      }
    }
  permit-command protocol-command-list;
  notification-options {
  type (message);
    custom-message [message];
  }
}
```

Hierarchy Level

[edit security utm feature-profile]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Configure UTM content-filtering features.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

content-filtering (utm-policy)

Syntax

```
content-filtering {
smtp-profile profile-name;
   pop3-profile profile-name;
}
```

Hierarchy Level

[edit security utm utm-policy *policy-name*]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Configure a UTM policy for the content-filtering protocols and attach this policy to a security profile to implement it.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

content-size

Syntax

content-size (log-and-permit | block);

Hierarchy Level

[edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus sophos-engine *profile-name* fallback-options]

Release Information

Statement introduced in Release 9.5 of Junos OS. Statement updated in Release 11.1 for Sophos Antivirus support.

Description

If the content size exceeds a set limit, the content is either passed or blocked. The default action is log-and-permit.

NOTE: When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. The default fallback action is log and permit, so you may want to change this option to block, in which case such a packet is dropped and a block message is sent to the client.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

content-size-limit

Syntax content-size-limit *value*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* scan-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

context

Syntax context *context-name* ;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Define the location of the signature where IDP should look for the attack in a specific Application Layer protocol.

Options *context-name* —Name of the context under which the attack has to be matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

context (Application-Level DDoS)

Syntax context *context-name*;

Hierarchy Level [edit security idp application–ddos *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the name of the application context that the IDP protocol decoder generates while parsing the application protocol from traffic data.

Options ***context-name***—Name of the protocol context under which the attack has to be matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

corrupt-file

Syntax corrupt-file (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Corrupt file is the error returned by the scan engine when engine detects a corrupted file. The default action is log-and-permit.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

count (Custom Attack)

Syntax count *count-value* ;

Hierarchy Level [edit security idp custom-attack *attack-name* time-binding]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the number of times that IDP detects the attack within the specified scope before triggering an event.

Options ***count-value*** —Number of times IDP detects the attack.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

count (Security Policies)

Syntax

```
count {
  alarm {
    per-minute-threshold number | per-second-threshold number ;
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable a count, in bytes or kilobytes, of all network traffic the security policy allows to pass through the device.

Options **per-minute-threshold** ***number*** —Alarm threshold in kilobytes per minute.

per-second-threshold ***number*** —Alarm threshold in bytes per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

crl

Syntax

```
crl {
  disable {
    on-download-failure;
  }
  refresh-interval hours ;
  url url-name ;
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name* revocation-check]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options

disable on-download-failure—(Optional) Override the default behavior and permit certificate verification even if the CRL fails to download.

refresh-interval *hours* —Time interval, in hours, between CRL updates.

url *url-name* —Name of the location from which to retrieve the CRL through HTTP or Lightweight Directory Access Protocol (LADP). You can specify one URL for each configured CA profile. By default, no location is specified. Use a fully qualified domain name (FQDN) or an IP address and, optionally, a port number. If no port number is specified, port 80 is used for HTTP and port 443 is used for LDAP.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

custom-attack

Syntax

```
custom-attack attack-name {
  attack-type {
    anomaly {
      direction (any | client-to-server | server-to-client);
      service service-name ;
      shellcode (all | intel | no-shellcode | sparc);
      test test-condition ;
    }
    chain {
      expression boolean-expression ;
      member member-name {
        attack-type {
          (anomaly | signature);
        }
      }
      order;
      protocol-binding {
        application application-name ;
        icmp;
        ip {
          protocol-number transport-layer-protocol-number ;
        }
        rpc {
          program-number rpc-program-number ;
        }
        tcp {
          minimum-port port-number maximum-port port-number ;
        }
        udp {
          minimum-port port-number maximum-port port-number ;
        }
      }
      reset;
      scope (session | transaction);
    }
    signature {
      context context-name ;
      direction (any | client-to-server | server-to-client);
      negate;
      pattern signature-pattern ;
      protocol {
        icmp {
          code {
            match (equal | greater-than | less-than | not-equal);
            value code-value ;
          }
          data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length ;
          }
          identification {
            match (equal | greater-than | less-than | not-equal);
```


Copyright © 2011, Juniper Networks, Inc.

```
        value identification-value ;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number ;
      }
      type {
        match (equal | greater-than | less-than | not-equal);
        value type-value ;
      }
    }
    ip {
      destination {
        match (equal | greater-than | less-than | not-equal);
        value hostname ;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value ;
      }
      ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
      }
      protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id ;
      }
      source {
        match (equal | greater-than | less-than | not-equal);
        value hostname ;
      }
      tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal ;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram ;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live ;
      }
    }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number ;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length ;
      }
      destination-port {
```

```
        match (equal | greater-than | less-than | not-equal);
        value destination-port ;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length ;
      }
      mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size ;
      }
      option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option ;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number ;
      }
      source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port ;
      }
      tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
      }
      urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
        value urgent-pointer ;
      }
      window-scale {
        match (equal | greater-than | less-than | not-equal);
        value window-scale-factor ;
      }
      window-size {
        match (equal | greater-than | less-than | not-equal);
        value window-size ;
      }
    }
    udp {
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length ;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port ;
      }
      source-port {
```


Copyright © 2011, Juniper Networks, Inc.

```
                match (equal | greater-than | less-than | not-equal);
                value source-port ;
              }
            }
          }
          protocol-binding {
            application application-name ;
            icmp;
            ip {
              protocol-number transport-layer-protocol-number ;
            }
            rpc {
              program-number rpc-program-number ;
            }
            tcp {
              minimum-port port-number maximum-port port-number ;
            }
            udp {
              minimum-port port-number maximum-port port-number ;
            }
          }
          regexp regular-expression ;
          shellcode (all | intel | no-shellcode | sparc);
        }
      }
      recommended-action (close | close-client | close-server | drop |
      drop-packet | ignore | none);
      severity (critical | info | major | minor | warning);
      time-binding {
        count count-value ;
        scope (destination | peer | source);
      }
    }
```

Hierarchy Level [edit security idp]

Release Information Statement modified in Release 9.3 of Junos OS.

Description Configure custom attack objects to detect a known or unknown attack that can be used to compromise your network.

Options *attack-name* —Name of the custom attack object.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

custom-attack-group

Syntax

```
custom-attack-group custom-attack-group-name {
  group-members [attack-group-name | attack-name];
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Configure custom attack group. A custom attack group is a list of attacks that would be matched on the traffic if the group is selected in a policy.

Options ***custom-attack-group-name*** —Name of the custom attack group.

The remaining statement is explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-attacks

Syntax custom-attacks [attack-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks], [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Select custom attacks defined under [edit security idp custom-attack] by specifying their names.

Options ***attack-name*** —Name of the new custom attack object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

custom-block-message

Syntax custom-block-message *value*;

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter a custom message to be sent when HTTP requests are blocked.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-message (antivirus notification-options fallback-block/non-block)

Syntax custom-message *message*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options fallback-block]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-message (content-filter notification-options)

Syntax custom-message *message*;

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Custom message notifications are generally used when content is blocked by the content filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-message-subject (antivirus notification-options fallback-block/non-block)

Syntax custom-message-subject *subject message*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options fallback-block]

Description Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

custom-message-subject (antivirus notification-options virus-detection)

Syntax custom-message-subject *subject message*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options virus-detection]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-message-subject (antivirus pattern-update email-notify)

Syntax custom-message-subject *subject message*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure the device to notify a specified administrator when patterns are updated. This is an email notification with a custom message and a custom subject line.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

custom-objects

Syntax

```
custom-objects {
filename-extension {
   value [list];
   }
   mime-pattern {
   value [list];
   }
   custom-url-category {
   value [list];
   }
   protocol-command {
   value [list];
   }
   url-pattern {
   value [list];
   }
}
```

Hierarchy Level [edit security utm]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure custom objects before configuring UTM feature-profile features.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

custom-tag-string

Syntax custom-tag-string [*string*];

Hierarchy Level [edit security utm feature-profile anti-spam sbl profile profile-name sbl-default-server]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a custom string for identifying a message as spam.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

custom-url-category

Syntax

```
custom-url-category {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

data-length

Syntax

```
data-length {
  match (equal | greater-than | less-than | not-equal);
  value data-length ;
}
```

Hierarchy Level
[edit security idp custom-attack *attack-name* attack-type signature protocol udp]
[edit security idp custom-attack *attack-name* attack-type signature protocol icmp]
[edit security idp custom-attack attack-name attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the number of bytes in the data payload. In the TCP header, for SYN, ACK, and FIN packets, this field should be empty.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***data-length*** —Match the number of bytes in the data payload.

Range: 0 through 65,535

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

datapath-debug

Syntax

```
datapath-debug {
  action-profile {
    event (jexec | lbt | mac-egress | mac-ingress | np-egress | np-ingress | pot)
      {
        count;
        packet-dump;
        packet-summary;
        trace;
      }
      module {
        flow {
          flag {
            all;
          }
        }
      }
      preserve-trace-order;
      record-pic-history;
  capture-file;
  packet-filter
    {
      action-profile (action-profile name | default) ;
      destination-port (port-range | protocol name );
      destination-prefix destination-prefix;
      protocol (protocol number | protocol name;
      source-port (port-range | protocol name);
      source-prefix source-prefix;
    }
  trace-options
    {
    file
      {
        filename;
        files filesnumber;
        match regular expression;
        size maximum file-size;
        (world-readable | no-world-readable);
      }
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Command introduced in Release 10.0 of Junos OS.

Description Configure the data path debugging options.

Options The remaining statements are explained separately.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

dead-peer-detection

Syntax

```
dead-peer-detection {
   always-send;
   interval seconds ;
   threshold number ;
}
```

Hierarchy Level
[edit security ike gateway *gateway-name*]

Release Information
Statement introduced in Release 8.5 of Junos OS.

Description
Enable the device to use dead peer detection (DPD). DPD is a method used by devices to verify the current existence and availability of IPsec peer devices. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to peers and waiting for DPD acknowledgements (R-U-THERE-ACK).

Options
The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

decompress-layer

Syntax

```
decompress-layer (log-and-permit | block);
```

Hierarchy Level
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Description
Decompress layer error is the error returned by the scan engine when the scanned file has too many compression layers. The default action is BLOCK.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

decompress-layer-limit

Syntax decompress-layer-limit *value*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* scan-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description The decompression layer limit specifies how many layers of nested compressed files and files with internal extractable objects, such as archive files (tar), the internal antivirus scanner can decompress before it executes the virus scan.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

default (antivirus fallback-options)

Syntax default (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

default (web-filtering fallback-settings)

Syntax

```
default (log-and-permit | block);
```

Hierarchy Level

[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper–local profile *profile-name* fallback-settings]

Description

All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

default-policy

Syntax

```
default-policy {
   (deny-all | permit-all);
}
```

Hierarchy Level

[edit security policies]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure the default security policy that defines the actions the device takes on a packet that does not match any user-defined policy.

Options

deny-all—Deny all traffic. Packets are dropped. This is the default.

permit-all—Permit all traffic that does not match a policy.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

default-rule (Application Firewall)

Syntax

```
default-rule {
   permit | deny;
}
```

Hierarchy Level [edit security application-firewall rule-set *rule-set-name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the default rule that defines the actions to be performed on a packet that does not match any defined rule.

Options ***permit***—Permit traffic that matches the rule.

deny—Deny the traffic. Packets are dropped.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

deny (Policy)

Syntax deny;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Block the service at the firewall. The device drops the packets.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

deny (SIP)

Syntax

```
deny {
  all | destination-ip address ;
  timeout seconds ;
}
```

Hierarchy Level [edit security alg sip application-screen protect]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Protect servers against INVITE attacks.

Options

all—Configure the Session Initiation Protocol (SIP) application screen to protect servers at all destination IP addresses against INVITE attacks.

destination-ip *address* —Configure the SIP application screen to protect the server at this destination IP address against INVITE attacks. You can include up to 16 destination IP addresses of servers to be protected. Enabling this option disables the all option.

timeout *seconds* —Amount of time (in *seconds*) to make an attack table entry for each INVITE, which is listed in the application screen.

Range: 1 through 3600 seconds

Default: 5 seconds

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

description (IDP Policy)

Syntax description *text* ;

Hierarchy Level
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name*]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify descriptive text for an exempt rule, or IPS rule.

Options *description* —Descriptive text about an exempt rule, or IPS rule.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

description (Security Policies)

Syntax description *description* ;

Hierarchy Level [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike policy *policy-name*],
[edit security ike proposal *proposal-name*],
[edit security ipsec policy *policy-name*],
[edit security ipsec proposal*proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify descriptive text for an IKE policy, IPsec policy, IKE proposal, or IPsec proposal.

Options ***description*** —Descriptive text about an IKE policy, IPsec policy, IKE proposal, or IPsec proposal.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

destination (Destination NAT)

Syntax

```
destination {
  pool pool-name {
    address < ip-address > (to ip-address | port port-number );
    routing-instance routing-instance-name ;
  }
  rule-set rule-set-name {
    from interface [interface-name] |
    routing-instance [routing-instance-name] | zone [zone-name];
    rule rule-name {
      match {
        destination-address destination-address ;
        destination-port port-number ;
        source-address [source-address];
      }
      then {
        destination-nat (off | pool pool-name );
      }
    }
  }
}
```

Hierarchy Level

[edit security nat]

Release Information

Statement modified in Release 9.6 of Junos OS.

Description

Configure destination NAT, which allows you to configure the following:

- Translate destination IP address or addresses to a specific IP address.
- Translate destination IP address or addresses and port number(s) to a specific IP address and one port number.
- Translate a range of destination IP addresses to another range of IP addresses. This mapping is one-to-one, static, and without PAT.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

destination (IP Headers in Signature Attack)

Syntax

```
destination {
   match (equal | greater-than | less-than | not-equal);
   value hostname ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the IP address of the attack target.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***host-name*** —Match an ip-address or a host name.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

destination-address (Destination NAT)

Syntax destination-address *destination-address* ;

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a destination address to match the rule. You can configure one address or a subnet.

NOTE:

- If the destination address is IPv4 and the pool is an IPv6 prefix, the length of the IPv6 prefix must be 96.
- If the destination address is an IPv6 prefix and the pool is an IPv6 prefix, their length must be the same.

Options ***destination-address*** —Destination address or a subnet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-address (IDP Policy)

Syntax destination-address [address-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

Description Specify a destination IP address or IP address set object to be used as the match destination address object. The default value is any.

Options ***address-name*** —IP address, IP address set object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-address (Security Policies)

Syntax

```
destination-address {
  address-name ;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description

Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

Options

address-name —IP address (**any**, **any-ipv4**, **any-ipv6**), IP address set, or address book entry, or wildcard address (represented as A.B.C.D/wildcard-mask).

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

destination-address (Security Policies Flag)

Syntax

```
destination-address {
   drop-translated;
   drop-untranslated;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information

Statement introduced in Release 9.2 of Junos OS.

Description

Specify whether the traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule or to packets where the destination IP address has not been translated.

On Juniper Networks security devices, destination NAT rules are processed before security policy lookup. Therefore, it is possible for a security policy to permit traffic from a source **S** to a destination **D** (where no destination NAT is performed) and also to permit traffic from the source **S** to the destination **d** (where **d** has been translated to **D**).

Options

drop-translated—Drop packets with translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has not been translated.

drop-untranslated—Drop packets without translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

destination-address (Source NAT)

Syntax destination-address [destination-address];

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a destination address to match the rule. You can configure multiple addresses or subnets.

Options ***destination-address*** —Destination address or a subnet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-address (Static NAT)

Syntax destination-address [destination-address];

Hierarchy Level [edit security nat static rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a destination address to match the rule. You can configure one address or a subnet.

Options ***destination-address*** —Destination address or a subnet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

destination-except

Syntax destination-except [address-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify a destination IP address or IP address set object to specify all destination address objects except the specified address objects. The default value is any.

Options ***address-name*** —IP address, IP address set object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-ip

Syntax destination-ip ***ip-address*** ;

Hierarchy Level [edit security ipsec vpn *vpn-name* vpn-monitor]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the destination of the Internet Control Message Protocol (ICMP) pings. If this statement is used, the device uses the peer's gateway address by default. (This statement is not supported on dynamic VPN implementations.)

Options ***ip-address*** —Destination IP address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

destination-ip-based

Syntax destination-ip-based *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can direct to a single destination IP address.

Options ***number*** —Maximum number of concurrent sessions that can be directed to a destination IP address.

Range: 1 through 50000

Default: 128

NOTE: For SRX Series devices, the applicable range is 1 through 8000000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-nat

Syntax destination-nat (off | pool *pool-name*);

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name* then]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the action of the destination NAT rule.

Options **off**—Do not perform destination NAT operation.

pool ***pool-name*** —Use user-defined destination NAT pool to perform destination NAT.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

destination-port (Destination NAT)

Syntax destination-port *port-number* ;

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a destination port to match the rule. You can configure one port.

Options ***port-number*** —Destination port number.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-port (Signature Attack)

Syntax

```
destination-port {
  match (equal | greater-than | less-than | not-equal);
  value destination-port ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol udp]
[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the port number of the attack target.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***destination-port*** —Match the port number of the attack target.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

destination-threshold

Syntax destination-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on the destination IP address, regardless of the destination port number.

Options *number* —Number of SYN segments received per second before the device begins dropping connection requests.

Range: 4 through 100,000 per second

Default: 2048 per second

NOTE: For SRX Series devices, the applicable range is 4 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

detect-shellcode

Syntax detect-shellcode;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable to detect the shell code and prevent buffer overflow attacks. By default this setting is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

detector

Syntax

```
detector {
  protocol-name protocol-name {
    tunable-name tunable-name {
      tunable-value protocol-value ;
    }
  }
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure protocol detector engine for a specific service.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

df-bit

Syntax df-bit (clear | copy | set);

Hierarchy Level [edit security ipsec vpn *vpn-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify how the router handles the Don't Fragment (DF) bit in the outer header.

Options

clear—Clear (disable) the DF bit from the outer header. This is the default.

copy—Copy the DF bit to the outer header.

set—Set (enable) the DF bit in the outer header.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

dh-group

Syntax dh-group (group1 | group2 | group5 | group14);

Hierarchy Level [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for dh-group group 14 is added in Release 11.1 of Junos OS.

Description Specify the IKE Diffie-Hellman group.

Options **dh-group**—Type of Diffie-Hellman prime modulus group for performing a Diffie-Hellman authentication key exchange.

- **group1**—768-bit algorithm.
- **group2**—1024-bit algorithm.
- **group5**—1536-bit algorithm.
- **group14**—2048-bit algorithm.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

direction (Custom Attack)

Syntax

direction (any | client-to-server | server-to-client);

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type anomaly]
[edit security idp custom-attack *attack-name* attack-type signature]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Define the connection direction of the attack.

Options

any—Detect the attack in either direction.

client-to-server—Detect the attack only in client-to-server traffic.

server-to-client—Detect the attack only in server-to-client traffic.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

direction (Dynamic Attack Group)

Syntax

```
direction {
   values [any | client-to-server | exclude-any | exclude-client-to-server |
   exclude-server-to-client | server-to-client];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a direction filter to add predefined attacks to the dynamic group based on the direction specified in the attacks.

Options **values**—Name of the direction filter. You can select from the following directions:

- **any**—Monitors traffic from client to server and server to client.
- **client-to-server**—Monitors traffic only from client to server (most attacks occur over **client-to-server** connections).
- **exclude-any**—Allows traffic from client to server and server to client.
- **exclude-client-to-server**—Allows traffic only from client to server.
- **exclude-server-to-client**—Allows traffic only from server-to-client.
- **server-to-client**—Monitors traffic only from server-to-client.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

disable-call-id-hiding

Syntax disable-call-id-hiding;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Disable translation of the host IP address in call-ID header. Translation is enabled by default.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

display-host (fallback-block)

Syntax display-host;

Hierarchy Level [edit security utm feature-profile anti-virus profile *profile name* notification-options fallback-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Display the computer host name in the notification e-mail sent to the administrator when a fallback-block notification occurs in Sophos antivirus.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

display-host (virus-detection)

Syntax display-host;

Hierarchy Level [edit security utm feature-profile anti-virus profile *profile name* notification-options virus-detection]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Display the computer host name in the notification e-mail sent to the administrator when a virus is detected by Sophos antivirus.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

distinguished-name

Syntax

```
distinguished-name {
   container  container-string ;
   wildcard  wildcard-string ;
}
```

Hierarchy Level

[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name* dynamic]

Release Information

Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description

Specify a distinguished name as the identifier for the remote gateway with a dynamic IP address. (This statement is not supported on dynamic VPN implementations.)

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

dns

Syntax

```
dns {
  disable;
  maximum-message-length number;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the Domain Name Service (DNS) Application Layer Gateway (ALG) on the device.

Options

disable—Disable the DNS ALG. By default, the DNS ALG is enabled. This option will enable or disable DNS ALG for both IPV4 and IPV6 mode.

maximum-message-length—A limit imposed on the size of individual DNS messages (see related section).

traceoptions—Configure DNS ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

download-profile (ftp antivirus utm-profile)

Syntax download-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus ftp]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

download-profile (ftp content-filtering utm-profile)

Syntax download-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering ftp]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

download-timeout

Syntax download-timeout *timeout* ;

Hierarchy Level [edit security idp security-package automatic]

Release Information Statement introduced in Release 9.6 R3 of Junos OS.

Description Specify the time that the device automatically times out and stops downloading the updated signature database from the specified URL.

NOTE: The default timeout is one minute. The process aborts with an error if the download does not finish before the specified timeout. It may be necessary to increase this value if security package updates are failing on timeouts.

Options ***download-timeout***—Time in minutes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

drop (gtp)

Syntax

```
drop {
aa-create-pdp {
   <0 | 1 | All>;
}
aa-delete-pdp {
   <0 | 1 | All>;
}
create pdp {
   <0 | 1 | All>;
}
data-record {
   <0 | 1 | All>;
}
delete-pdp {
   <0 | 1 | All>;
}
echo {
   <0 | 1 | All>;
}
error-indication {
   <0 | 1 | All>;
}
failure-report {
   <0 | 1 | All>;
}
fwd-relocation {
   <0 | 1 | All>;
}
fwd-srns-context {
   <0 | 1 | All>;
}
g-pdu {
   <0 | 1 | All>;
}
identification {
   <0 | 1 | All>;
}
node-alive {
   <0 | 1 | All>;
}
note-ms-present {
   <0 | 1 | All>;
}
pdu-notification {
   <0 | 1 | All>;
}
ran-info {
   <0 | 1 | All>;
}
redirection {
   <0 | 1 | All>;
}
```


Copyright © 2011, Juniper Networks, Inc.

```
relocation-cancel {
   <0 | 1 | All>;
}
send-route {
   <0 | 1 | All>;
}
sgsn-context {
   <0 | 1 | All>;
}
supported-extension {
   <0 | 1 | All>;
}
update-pdp {
   <0 | 1 | All>;
}
ver-not-supported {
   <0 | 1 | All>;
}
```

Hierarchy Level [edit security gprs gtp profile *profile name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Display information about the configuration of the current GTP inspection.

- *number*—Specify the GTP release version number for the specified message type. The possible versions are 0 (for GTP 97) or 1 (GTP 99). You must select 0, 1, or all, or you will receive a syntax error.

The following lists CLI keywords that each represent a GTP message type. A GTP message type includes one or many messages. When you set or delete a message type, you automatically permit or deny access to all messages of the specified type.

- **aa-create-pdp** Represents Create AA PDP Context Request and Create AA PDP Context Response messages.
- **aa-delete-pdp** Represents Delete AA PDP Context Request and Delete AA PDP Context Response messages.
- **create-pdp** Represents Create PDP Context Request and Create PDP Context Response messages.
- **data-record** Represents Data Record request and Data Record response messages.
- **delete-pdp** Represents Delete PDP Context Request and Delete PDP Context Response messages.
- **echo** Represents Echo Request and Echo Response messages.
- **error-indication** Represents Error Indication messages.
- **failure-report** Represents Failure Report Request and Failure Report Response messages.
- **fwd-relocation** Represents Forward Relocation Request, Forward Relocation Response, Forward Relocation Complete, and Forward Relocation Complete Acknowledge messages.
- **fwd-srns-context** Represents Forward SRNS Context Request and Forward SRNS Context Response messages.
- **g-pdu** Represents G-PDU and T-PDU messages.
- **identification** Represents Identification Request and Identification Response messages.
- **node-alive** Represents Node Alive Request and Node Alive Response messages.
- **note-ms-present** Represents Note MS GPRS Present Request and Note MS GPRS Present Response messages.
- **pdu-notification** Represents PDU Notification request and PDU Notification response messages.
- **ran-info** Represents Ran Info relay messages.
- **redirection** Represents Redirection request and Redirection response messages.
- **relocation-cancel** Represents Relocations Cancel request and Relocation Cancel response messages.
- **send-route** Represents Send Route info request and Send Route info response messages.

 Copyright © 2011, Juniper Networks, Inc.

- **sgsn-context** Represents SGSN Context request and SGSN Context response messages.
- **supported-extension** Represents Supported Extension headers notification messages.
- **update-pdp** Represents Update PDP request and Update PDP response messages.
- **ver-not-supported** Represents Version Not Supported messages.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

drop (SCTP)

Syntax

```
drop {
  m3ua-service {
    isup;
    sccp;
    tup;
  }
  payload-protocol {
    all;
    asap;
    bicc;
    ddp-segment;
    ddp-stream;
    dua;
    enrp;
    h248;
    h323;
    iua;
    m2pa;
    m2ua;
    m3ua;
    qipc;
    simco;
    sua;
    tali;
    v5ua;
  }
}
```

Hierarchy Level [edit security gprs sctp profile *name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Display information about the configuration of the current Stream Control Transmission Protocol (SCTP) inspection.

Options **m3ua-services**—M3UA data service indicator. The following values are supported:

- **isup**—ISDN Upper Part.
- **sccp**—Signaling Connection Control Part.
- **tup**—Telephone User Part.

payload-protocol—SCTP payload protocol identifier. The following values are supported.

- **all**—All SCTP payload protocol identifiers (id:1~17).
- **asap**—Aggregate Server Access Protocol.
- **bicc**—Bearer Independent Call Control.
- **ddp-segement**—Direct Data Placement Segment chunk.
- **ddp-stream**—Direct Data Placement Stream session control.

Copyright © 2011, Juniper Networks, Inc.

- **dua**—DPNSS/DASS 2 extensions to IUA Protocol.
- **enrp**—Endpoint Handle escape Redundancy Protocol.
- **h248**—H.248 Protocol.
- **h323**—H.323 Protocol.
- **iua**—ISDN User Adaptation Layer.
- **m2pa**—MTP2 User Peer-to-Peer Adaption Layer.
- **m2ua**—MTP2 User Adaption Layer.
- **m3ua**—MTP3 User Adaption Layer.
- **qipc**—Q.IPC.
- **simco**—Simple Middlebox Configuration.
- **sua**—SCCP User Adaption Layer.
- **tali**—Transport Adapter Layer Interface.
- **v5ua**—v5.2 User Adaption Layer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

dynamic

Syntax

```
dynamic {
  connections-limit number;
    distinguished-name {
    container container-string;
    wildcard wildcard-string;
    }
    hostname domain-name;
    ike-user-type (group-ike-id | shared-ike-id);
    inet ip-address;
    inet6 ipv6-address;
  user-at-hostname user-at-hostname;
```

Hierarchy Level

[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS. The **inet6** option is not supported on the **group-vpn** hierarchies.

Description

Specify the identifier for the remote gateway with a dynamic IPv4 or IPv6 address. Use this statement to set up a VPN with a gateway that has an unspecified IPv4 or IPv6 address.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

dynamic-application

Syntax

dynamic-application [***dynamic-application-names***];

Hierarchy Level

[edit security application-firewall rule-sets ***rule-set-name*** rule ***rule-name*** match]

Release Information

Statement introduced in Release 11.1 of Junos OS.

Description

Specify the dynamic application name to match.

Options

dynamic-application-names—Set of dynamic application names.

Usage Guidelines

For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

dynamic-vpn

Syntax

```
dynamic-vpn {
   access-profile profile-name;
   force-upgrade;
   clients {
      configuration-name {
         remote-protected-resources {
            ip-address/mask;
         }
         remote-exceptions {
            ip-address/mask;
         }
         ipsec-vpn configuration-name;
         user {
            username;
         }
      }
   }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to configure the dynamic VPN feature. The dynamic VPN feature simplifies remote access by enabling users to create IPsec VPN tunnels without having to manually configure settings on their PCs or laptops. Instead, authenticated users can simply download a preconfigured Web client to their computers with all the client-side information required to create and manage an IPsec VPN tunnel to the server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

dynamic-attack-group

Syntax

```
dynamic-attack-group dynamic-attack-group-name {
  filters {
    category {
      values [list-of-values];
    }
    direction {
      values [any | client-to-server | exclude-any | exclude-client-to-server |
      exclude-server-to-client | server-to-client];
    }
    false-positives {
      values [frequently | occasionally | rarely | unknown];
    }
    performance {
      values [fast | normal | slow | unknown];
    }
    products {
      values [list-of-values];
    }
    recommended;
    service {
      values [list-of-values];
    }
    severity {
      values [critical | info | major | minor | warning];
    }
    type {
      values [anomaly | signature];
    }
  }
}
```

Hierarchy Level

[edit security idp]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Configure dynamic attack group. Dynamic attack groups select its members based on the filters specified in the group. Hence the list of attacks get updated (added or removed) when a new signature database is used.

Options

dynamic-attack-group-name —Name of the dynamic attack group.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

early-ageout

Syntax early-ageout *seconds* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define the ageout value before the device aggressively ages out a session from its session table.

Options ***seconds*** —Amount of time that elapses before the device aggressively ages out a session.

Range: 1 through 65,535 seconds

Default: 20 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

email-notify

Syntax

```
email-notify {
admin-email email address
   custom-message message
   custom-message-subject message subject
}
```

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

enable-all-qmodules

Syntax (enable-all-qmodules | no-enable-all-qmodules);

Hierarchy Level [edit security idp sensor-configuration global]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable all the qmodules of the global rulebase IDP security policy. By default all the qmodules are enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

enable-packet-pool

Syntax (enable-packet-pool | no-enable-packet-pool);

Hierarchy Level [edit security idp sensor-configuration global]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable the packet pool to use when the current pool is exhausted. By default packet pool is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

encryption

Syntax

```
encryption {
   algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
   key (ascii-text  key  | hexadecimal  key  );
}
```

Hierarchy Level

[edit security ipsec vpn *vpn-name* manual]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Configure an encryption algorithm and key for a manual Security Association (SA). (This statement is not supported on dynamic VPN implementations.)

Options

algorithm—Type of encryption algorithm. It can be one of the following:

- **des-cbc**—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
- **3des-cbc**—Has block size of 8 bytes (64 bits); its key size is 192 bits long

NOTE: For 3des-cbc, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.

- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

key—Type of encryption key. It can be one of the following:

- **ascii-text key**—ASCII text key. For the **des-cbc** option, the key contains 8 ASCII characters; for **3des-cbc**, the key contains 24 ASCII characters.
- **hexadecimal key**—Hexadecimal key. For the **des-cbc** option, the key contains 16 hexadecimal characters; for the **3des-cbc** option, the key contains 48 hexadecimal characters.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

encryption-algorithm

Syntax encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);

Hierarchy Level [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Configure an IKE encryption algorithm.

Options **3des-cbc**—Has a block size of 24 bytes; the key size is 192 bits long.

des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.

aes-128-cbc—Advanced Encryption Standard (AES) 128-bit encryption algorithm.

aes-192-cbc—Advanced Encryption Standard (AES) 192-bit encryption algorithm.

aes-256-cbc—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

endpoint-registration-timeout

Syntax endpoint-registration-timeout *seconds* ;

Hierarchy Level [edit security alg h323]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the timeout value in seconds for entries in the NAT table.

Options *seconds* —Timeout value.
Range: 10 through 50000 seconds
Default: 3600 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

engine-not-ready

Syntax

engine-not-ready (log-and-permit | block);

Hierarchy Level

[edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting. The default action is BLOCK.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

enrollment

Syntax

```
enrollment {
   retry number ;
   retry-interval seconds ;
   url url-name ;
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the enrollment parameters for a certificate authority (CA).

Options

retry ***number*** —Number of automated attempts for online enrollment to be retried in case enrollment response is pending.

Range: 0 through 1080

Default: 10

retry-interval ***seconds*** —Time interval, in seconds, between the enrollment retries.

Range: 0 through 3600

Default: 900 seconds

url ***url-name*** —Enrollment URL where the Simple Certificate Enrollment Protocol (SCEP) request is sent to the certification authority (CA) as configured in this profile.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

establish-tunnels

Syntax establish-tunnels (immediately | on-traffic);

Hierarchy Level [edit security ipsec vpn *vpn-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify when IKE is activated: immediately after VPN information is configured and configuration changes are committed, or only when data traffic flows. In the second case, IKE needs to be negotiated with the peer gateway.

Options **immediately**—IKE is activated immediately after VPN configuration and configuration changes are committed.

on-traffic—IKE is activated only when data traffic flows and must to be negotiated.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

event-rate

Syntax Syntax event-rate *rate*

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Limits the rate (0 to 1500) at which logs will be streamed per second.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

exception (antivirus mime-whitelist)

Syntax exception *listname*;

Hierarchy Level [edit security utm feature-profile anti-virus mime-whitelist list *listname*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

exception (content-filter block-mime)

Syntax exception *listname*;

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name* block-mime list *list-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the content-filter to use an exception list to the MIME block list (custom objects).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

exclude-context-values

Syntax

```
context <context-name> {
   exclude-context-values regular-expression-1... regular-expression-n;
}
```

Hierarchy Level

[edit security idp application–ddos *name* **context** *context-name*]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure a list of common context value patterns that should be excluded from application-level distributed denial-of-service (DDoS) detection. For example, if you have a webserver that receives a high number of HTTP requests on home/landing page, you can exclude it from application-level DDoS detection.

Options

regular-expression —List of patterns for exclusion. Example: **www.juniper.net** **www.acmegizmo.com**.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

expression

Syntax expression *boolean-expression*;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type chain]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Configure Boolean expression. The Boolean expression defines the condition for the individual members of a chain attack that will decide if the chain attack is hit.

For standalone IDP devices, expression overrides order function.

For SRX Series devices, expression and order cannot be configured together. Only one of them can be specified.

Options ***boolean-expression***—Boolean operators:

- **or**—If either of the member name patterns match, the expression matches.
- **and**—If both of the member name patterns match, the expression matches. It does not matter which order the members appear in.
- **oand**—If both of the member name patterns match, and if they appear in the same order as in the Boolean Expression, the expression matches.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

external-interface (IKE Gateway)

Syntax external-interface ***external-interface-name*** ;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the outgoing interface for IKE SAs. This interface is associated with a zone that acts as its carrier, providing firewall security for it.

Options ***external-interface-name*** —Name of the interface to be used to send traffic to the IPsec VPN.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

external-interface (Manual Security Association)

Syntax external-interface *external-interface-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* manual]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the outgoing interface for the manual SA. (This statement is not supported on dynamic VPN implementations.)

Options *external-interface-name* —Name of the outgoing interface.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

fallback-block

Syntax

```
fallback-block {
custom-message;
   custom-message-subject;
   notify-mail-sender;
   type;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure notifications for both fallback blocking and fallback nonblocking actions. Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

fallback-block (Sophos antivirus notification-options)

Syntax

```
fallback-block {
   administrator-email email address;
   allow-email;
   custom-message message;
   custom-message-subject subject;
   display-host;
   no-notify-mail-sender;
   notify-mail-sender;
   type (message | protocol-only);
}
```

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine *profile-name* notification-options]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description You can configure notifications for both fallback blocking and fallback non-blocking actions. Fallback options instruct the system how to handle errors returned by the Sophos scan engine.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

fallback-options (antivirus juniper-express-engine)

Syntax

```
fallback-options {
default (log-and-permit | block);
   content-size (log-and-permit | block);
   engine-not-ready (log-and-permit | block);
   timeout (log-and-permit | block);
   out-of-resources (log-and-permit | block);
   too-many-requests (log-and-permit | block);
}
```

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Fallback options tell the system how to handle the errors.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

fallback-options (antivirus kaspersky-lab-engine)

Syntax

```
fallback-options {
default (log-and-permit | block);
   corrupt-file (log-and-permit | block);
   password-file (log-and-permit | block);
   decompress-layer (log-and-permit | block);
   content-size (log-and-permit | block);
   engine-not-ready (log-and-permit | block);
   timeout (log-and-permit | block);
   out-of-resources (log-and-permit | block);
   too-many-requests (log-and-permit | block);
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name*]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

fallback-options (antivirus sophos-engine)

Syntax

```
fallback-options {
   content-size (block | log-and-permit | permit);
   default (block | log-and-permit | permit);
   engine-not-ready (block | log-and-permit | permit);
   out-of-resource (block | log-and-permit | permit);
   timeout (block | log-and-permit | permit);
   too-many-requests (block | log-and-permit | permit);
}
```

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine *profile name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure fallback options to instruct the system how to handle errors.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

fallback-settings (web-filtering surf-control-integrated)

Syntax

```
fallback-settings {
default (log-and-permit | block);
   server-connectivity (log-and-permit | block);
   timeout (log-and-permit | block);
   too-many-requests (log-and-permit | block);
}
```

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

fallback-settings (web-filtering websense-redirect)

Syntax

```
fallback-settings {
default (log-and-permit | block);
   server-connectivity (log-and-permit | block);
   timeout (log-and-permit | block);
   too-many-requests (log-and-permit | block);
}
```

Hierarchy Level [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

fallback-settings (web-filtering juniper-local)

Syntax

```
fallback-settings {
default (log-and-permit | block);
   too-many-requests (log-and-permit | block);
}
```

Hierarchy Level [edit security utm feature-profile web-filtering juniper–local profile *profile-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

false-positives

Syntax

```
false-positives {
   values [frequently | occasionally | rarely | unknown];
}
```

Hierarchy Level

[edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify a false-positives filter to add attack objects based on the frequency that the attack produces a false positive on your network.

Options

values—Name of the false positives filter. You can select from the following false positives frequency:

- **frequently**—Frequently track false positives occurrence.
- **occasionally**—Occasionally track false positives occurrence.
- **rarely**—Rarely track false positives occurrence.
- **unknown**—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track false positives.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

family

Syntax

```
family {
  inet6 {
    mode (packet-based | flow-based | drop ); default: drop
  }
  iso {
    mode packet-based;
  }
  mpls {
    mode packet-based;
  }
}
```

Hierarchy Level [edit security forwarding-options]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Determine the protocol family to be used for packet forwarding.

Options The remaining statements are explained separately.

NOTE: The **iso** and **mpls** family statements are not applicable for SRX3400, SRX3600, SRX5400, or SRX5600, which do not support packet-based mode. The **iso** and **mpls** statements do not appear in the CLI for these devices.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

feature-profile

Syntax

```
feature-profile {
anti-virus {
  type kaspersky-lab-engine;
    kaspersky-lab-engine {
    pattern-update {
      url;
        interval value;
      }
      profile profile-name {
      fallback-options {
        default (log-and-permit | block);
          corrupt-file (log-and-permit | block);
          password-file (log-and-permit | block);
          decompress-layer (log-and-permit | block);
          content-size (log-and-permit | block);
          engine-not-ready (log-and-permit | block);
          timeout (log-and-permit | block);
          out-of-resources (log-and-permit | block);
          too-many-requests (log-and-permit | block);
        }
        scan-options {
        intelligent-prescreening;
          scan-mode (scan-all | by--extension);
          content-size-limit value;
          timeout value;
          decompress-layer-limit value;
        }
        notification-options {
        virus-detection {
          type (message | protocol-only);
            notify-mail-sender;
            custom-message;
          }
          fallback-block {
          custom-message;
            notify-mail-sender;
            type;
          }
        }
        trickling {
          timeout value;
        }
      }
    }
    type juniper-express-engine;
    juniper-express-engine {
    pattern-update {
      url;
        interval value;
      }
      profile profile-name {
      fallback-options {
```

```
            default (log-and-permit | block);
              content-size (log-and-permit | block);
              engine-not-ready (log-and-permit | block);
              timeout (log-and-permit | block);
              out-of-resources (log-and-permit | block);
              too-many-requests (log-and-permit | block);
            }
            scan-options {
            intelligent-prescreening;
              scan-mode (scan-all | by--extension);
              content-size-limit value;
              timeout value;
              decompress-layer-limit value;
            }
            notification-options {
            virus-detection {
              type (message | protocol-only);
                notify-mail-sender;
                custom-message;
              }
              fallback-block {
              custom-message;
                notify-mail-sender;
                type;
              }
            }
            trickling {
              timeout value;
            }
          }
          mime-whitelist {
          list listname {
            exception listname;
          }
          url-whitelist {
          listname;
          }
        }
      }
      web-filtering {
      surf-control-integrated {
        cache {
          timeout value;
          }
          server {
          host host-name;
            port number;
          }
        profile profile-name{
          default (log-and-permit | block);
            custom-block-message value;
            fallback-settings {
            default (log-and-permit | block);
              server-connectivity (log-and-permit | block);
              timeout (log-and-permit | block);
              too-many-requests (log-and-permit | block);
```

 Copyright © 2011, Juniper Networks, Inc.

```
            }
            category customurl-list name {
            action (log-and-permit | block);
            }
          }
        websense-redirect {
        profile profile-name {
        server {
          host host-name;
            port number;
          }
          sockets value;
            timeout value;
            fallback-settings {
            default (log-and-permit | block);
              server-connectivity (log-and-permit | block);
              timeout (log-and-permit | block);
              too-many-requests (log-and-permit | block);
            }
          }
        url-whitelist {
        listname;
        }
        url-blacklist {
        listname;
        }
      }
      anti-spam {
      sbl {
        profile profile-name{
          sbl-default-server;
            spam-action (log-and-permit | block);
            custom-tag-string [***SPAM***];
          }
          address-whitelist{
          listname;
          }
        }
      }
      content-filter {
      profile profile-name{
        block-command protocol-command-list;
          block-content-type (java-applet | exe | http-cookie);
          block-mime {
          list list-name {
            exception list-name;
            }
          }
        permit-command protocol-command-list;
        notification-options {
        type (message | protocol-only);
          custom-message [message];
        }
      }
    }
```

Hierarchy Level [edit security utm]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

filename-extension

Syntax

```
filename-extension {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

filters

Syntax

```
filters {
  category {
    values [list-of-values];
  }
  direction {
    values [any | client-to-server | exclude-any | exclude-client-to-server |
    exclude-server-to-client | server-to-client];
  }
  false-positives {
    values [frequently | occasionally | rarely | unknown];
  }
  performance {
    values [fast | normal | slow | unknown];
  }
  products {
    values [list-of-values];
  }
  recommended;
  service {
    values [list-of-values];
  }
  severity {
    values [critical | info | major | minor | warning];
  }
  type {
    values [anomaly | signature];
  }
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description To create a dynamic attack group, set the criteria using the different type of filters.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

fin-no-ack

Syntax fin-no-ack;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of an illegal combination of flags, and reject packets that have this combination.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

firewall-authentication (Policies)

Syntax

```
firewall-authentication {
  pass-through {
    access-profile profile-name ;
    client-match match-name ;
    web-redirect;
  }
  web-authentication {
    client-match user-or-group ;
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure firewall authentication methods.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

firewall-authentication (Security)

Syntax

```
firewall-authentication {
  traceoptions {
    flag {
      all <detail | extensive | terse>;
      authentication <detail | extensive | terse>;
      proxy <detail | extensive | terse>;
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define data-plane firewall authentication tracing options.

Options flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Enable all tracing operations.
- **authentication**—Trace data-plane firewall authentication events.
- **proxy**—Trace data-plane firewall authentication proxy events.

detail—Display moderate amount of data.

extensive—Display extensive amount of data.

terse—Display minimum amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

first-update

Syntax first-update;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Generate an AppTrack start message when a new session begins. (A final message is produced at session end with any option.) This option overrides the **first-update-interval** option if both are specified.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

first-update-interval

Syntax first-update-interval *minutes*;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description For long-lived sessions being monitored by AppTrack, configure this value to send the first update message earlier than the session update interval specifies.

NOTE: The **first-update-interval** setting is disregarded if the **first-update** option is set to log the first message at session start.

Options ***minutes***—Maximum number of minutes after session start for the first update message to be sent. This value must be smaller than the **session-update-interval** setting.

Default: 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

flood (ICMP)

Syntax

```
flood {
  threshold number ;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the device to detect and prevent Internet Control Message Protocol (ICMP) floods. An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Options

threshold *number* —Number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

Range: 1 through 100000 per second

Default: 1000 per second

NOTE: For SRX Series devices the applicable range is 1 through 4000000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

flood (UDP)

Syntax

```
flood {
   threshold number ;
}
```

Hierarchy Level

[edit security screen ids-option *screen-name* udp]

Release Information

Statement modified in Release 9.2 of Junos OS.

Description

Configure the device to detect and prevent UDP floods. UDP flooding occurs when an attacker sends UDP packets to slow down the system to the point that it can no longer process valid connection requests.

The threshold defines the number of UDP packets per second allowed to ping the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options

threshold ***number*** —Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.

Range: 1 through 100000 per second

Default: 1000 per second

NOTE: For SRX series devices the applicable range is 1 through 4000000 per second.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

flow (IDP)

Syntax

```
flow {
   (allow-icmp-without-flow | no-allow-icmp-without-flow);
   (log-errors | no-log-errors);
   max-timers-poll-ticks value ;
   reject-timeout value ;
   (reset-on-policy | no-reset-on-policy);
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure the IDP engine to manage the packet flow.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

flow (Security Flow)

Syntax

```
flow {
  aging {
    early-ageout seconds ;
    high-watermark percent ;
    low-watermark percent ;
  }
  allow-dns-reply;
  bridge {
    block-non-ip-all;
    bypass-non-ip-unicast;
    no-packet-flooding {
      no-trace-route;
    }
  }
  route-change-timeout seconds ;
  syn-flood-protection-mode (syn-cookie | syn-proxy);
  tcp-mss {
    all-tcp {
      mss value ;
    }
    gre-in {
      mss value ;
    }
    gre-out {
      mss value ;
    }
    ipsec-vpn {
      mss value ;
    }
  }
  tcp-session {
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    tcp-initial-timeout seconds ;
  }
  traceoptions {
    file filename <files number > <size maximum-file-size >;
    <world-readable | no-world-readable>;
    flag flag;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

Copyright © 2011, Juniper Networks, Inc.

- Enable or disable DNS replies when there is no matching DNS request.
- Set the initial session-timeout values.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

force-upgrade

Syntax force-upgrade;

Hierarchy Level [edit security dynamic-vpn]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to force users to automatically upgrade the Access Manager when newer versions are available. If you include this statement in your configuration, it is automatically enabled. If the statement is not present in your configuration, the force upgrade option is not enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

format (first use in Security Logging)

Syntax format (syslog | sd-syslog)

Hierarchy Level [edit security log]

Release Information Statement introduced in a release of Junos OS prior to Release 10.0.

Description Set the default security log format of logging to **syslog** (system log) or **sd-syslog** (structured system log).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

format (second use in Security Logging)

Syntax format (syslog | sd-syslog | welf)

Hierarchy Level [edit security log stream]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set the format of logging to **syslog** (system log), **sd-syslog** (structured system log), or **welf**. Note that for the WELF format, the category must be set to **content-security** (see **category (Security Logging)**).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

forwarding-options

Syntax

```
forwarding-options {
  family {
    inet6 {
      mode (packet-based | flow-based | drop ); default: drop
    }
    iso {
      mode packet-based;
    }
  }
  mpls {
    mode packet-based;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Determine how the **inet6, iso**, and **mpls** protocol families manage security forwarding options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

forwarding-process

Syntax

```
forwarding-process {
  application-services {
    maximize-idp-sessions {
      weight {
        equal;
        firewall;
        idp;
      }
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

fragment

Syntax fragment;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and drop any ICMP frame with the More Fragments flag set or with an offset indicated in the **offset** field.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

from

Syntax
from interface [interface-name] |
routing-instance [routing-instance-name] | zone [zone-name];

Hierarchy Level
[edit security nat destination rule-set *rule-set-name*],
[edit security nat source rule-set *rule-set-name*],
[edit security nat static rule-set *rule-set-name*]

Release Information
Statement modified in Release 9.3 of Junos OS.

Description
Specify the source of the packet among the routing instance, interface, or zone.

Options
interface ***interface-name*** —Name of the interface.

routing-instance ***routing-instance-name*** —Name of the routing instance.

zone ***zone-name*** —Name of the zone.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

from-zone (IDP Policy)

Syntax
from-zone ***zone-name*** ;

Hierarchy Level
[edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information
Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Junos OS 10.0.

Description
Specify a source zone to be associated with the security policy. The default value is any.

Options
zone-name —Name of the source zone object.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

from-zone (Security Policies)

Syntax

```
from-zone zone-name to-zone zone-name {
  policy policy-name {
    match {
      application [ application-name-or-set ];
      destination-address {
        address-name ;
      }
      source-address {
        address-name ;
      }
    }
    scheduler-name scheduler-name ;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number ;
        }
      }
      (deny | reject);
      permit {
        application-services (redirect-wx | reverse-redirect-wx);
        application-firewall {
          rule-set rule-set-name;
        }
        destination-address {
          drop-translated;
          drop-untranslated;
        }
        firewall-authentication {
          pass-through {
            access-profile profile-name ;
            client-match match-name ;
            web-redirect;
          }
          web-authentication {
            client-match user-or-group ;
          }
        }
        tunnel {
          ipsec-group-vpn group-vpn;
          ipsec-vpn vpn-name ;
          pair-policy pair-policy ;
        }
      }
      log {
        session-close;
        session-init;
      }
    }
  }
}
```

Hierarchy Level [edit security policies]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a source zone and destination zone to be associated with the security policy.

Options ***zone-name*** —Name of the source zone.

to-zone ***zone-name*** —Name of the destination zone.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ftp

Syntax

```
ftp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the FTP ALG on the device.

Options

disable—Disable the FTP ALG. By default, the FTP ALG is enabled. This option will enable or disable DNS ALG for both IPV4 and IPV6 mode.

NOTE: By default, FTP ALG is disabled for SRX Series devices.

traceoptions—Configure FTP ALG tracing options. To specify more than one trace operation, include multiple flag statements.

flag—Trace operation to perform.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ftp (content-filtering utm-policy)

Syntax

```
ftp {
upload-profile profile-name;
  download-profile profile-name;
}
```

Hierarchy Level

[edit security utm utm-policy *policy-name* content-filtering]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Configure a UTM policy for the content-filtering FTP protocol and attach this policy to a security profile to implement it.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

functional-zone

Syntax

```
functional-zone {
  management {
    host-inbound-traffic {
      protocols {
        protocol-name ;
        protocol-name <except>;
      }
      system-services {
        service-name ;
        service-name <except>;
      }
    }
    interfaces interface-name {
      host-inbound-traffic {
        protocols {
          protocol-name ;
          protocol-name <except>;
        }
        system-services {
          service-name ;
          service-name <except>;
        }
      }
    }
    screen screen-name ;
  }
}
```

Hierarchy Level [edit security zones]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure a functional zone.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

gatekeeper

Syntax gatekeeper threshold *rate* ;

Hierarchy Level [edit security alg h323 application-screen message-flood]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the rate at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped.

Options **threshold** *rate* —Threshold measured in messages per second.

Range: 1 through 50000

Default: 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

gateway (IKE)

Syntax

```
gateway gateway-name {
  address [( ip-address | hostname )] |
  dead-peer-detection {
    always-send;
    interval seconds ;
    threshold number ;
  }
  dynamic {
    connections-limit number ;
    distinguished-name {
      container container-string ;
      wildcard wildcard-string ;
    }
    hostname domain-name ;
    ike-user-type (group-ike-id | shared-ike-id);
    inet ip-address ;
    inet6 ipv6-address ;
    user-at-hostname user-at-hostname ;
  }
  external-interface external-interface-name ;
  ike-policy name ;
  local-identity (hostname hostname | inet ip-address | inet6 ipv6-address |
  user-at-hostname e-mail-address | distinguished-name string );
  nat-keepalive seconds ;
  no-nat-traversal;
  xauth {
    access-profile profile-name ;
  }
}
```

Hierarchy Level

[edit security group-vpn member ike]
[edit security group-vpn server ike]
[edit security ike]

Release Information

Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS. The **inet6** option is not supported on the **group-vpn** hierarchies.

Description

Configure an IKE gateway.

Options

gateway-name —Name of the gateway.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

gateway (Manual Security Association)

Syntax gateway *ip-address* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* manual]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description For a manual security association, specify the IPv4 or IPv6 address of the peer. (This statement is not supported on dynamic VPN implementations.)

Options ***ip-address*** —IPv4 or IPv6 address of the peer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

general-ikeid

Syntax general-ikeid;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Accept general peer IKE ID.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

global

Syntax

```
global {
   (enable-all-qmodules | no-enable-all-qmodules);
   (enable-packet-pool | no-enable-packet-pool);
   (policy-lookup-cache | no-policy-lookup-cache);
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure the global rulebase IDP security policy.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

gre-in

Syntax

```
gre-in {
   mss value ;
}
```

Hierarchy Level [edit security flow tcp-mss]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable and specify the TCP maximum segment size (TCP MSS) for Generic Routing Encapsulation (GRE) packets that are coming out from an IPsec VPN tunnel. If the device receives a GRE-encapsulated TCP packet with the SYN bit and TCP MSS option set and the TCP MSS option specified in the packet exceeds the TCP MSS specified by the device, the device modifies the TCP MSS value accordingly. By default, a TCP MSS for GRE packets is not set.

Options **mss** *value* —TCP MSS for GRE packets. Value is optional.

Range: 64 through 63535 bytes

Default: 1320 bytes, if no value is specified

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

gre-out

Syntax

```
gre-out {
  mss value ;
}
```

Hierarchy Level

[edit security flow tcp-mss]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Enable and specify the TCP maximum segment size (TCP MSS) for Generic Routing Encapsulation (GRE) packets that are going into an IPsec VPN tunnel. If the device receives a GRE-encapsulated TCP packet with the SYN bit and TCP MSS option set and the TCP MSS option specified in the packet exceeds the TCP MSS specified by the device, the device modifies the TCP MSS value accordingly. By default, a TCP MSS for GRE packets is not set.

Options

mss *value* —TCP MSS for GRE packets. Value is optional.

Range: 64 through 65,535 bytes

Default: 1320 bytes

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

group (Group VPN Server)

Syntax

```
group name{
  activation-time-delay seconds;
  anti-replay-time-window seconds;
  description text;
  group-id number;
  ike-gateway gateway-name;
  ipsec-sa name {
    proposal name;
      match-policy name {
        destination ip-address/netmask;
        destination-port number;
        protocol number;
        source ip-address/netmask;
        source-port number;
    }
  }
  no-anti-replay;
  server-address ip-address;
  server-member-communication {
    certificate certificate-id;
    communication-type (multicast | unicast);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    heartbeat seconds;
    lifetime-seconds seconds;
    multicast-group address;
    multicast-outgoing-interface interface;
    number-of-retransmission number;
    retransmission-period seconds;
    sig-hash-algorithm (md5 | sha1);
  }
}
```

Hierarchy Level [edit security group-vpn server]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure group VPN on the group server.

Options **activation-time-delay**—Time, in seconds, before a group member can use a new key when a member reregisters with the group server. When a member registers for the first time with the server (the member does not have a key), there is no delay. When the server sends a rekey message to the member, the member waits twice the **activation-time-delay** value before using the new key. Specify a value from 10 to 900. The default is 15 seconds.

NOTE: The lifetime-seconds values of all IPsec SA proposals and of the server-member-communication in the group must be at least 10 times the activation-time-delay value.

anti-replay-time-window—Configure antireplay time in seconds. Specify a value from 60 to 360. The default is 100 seconds.

description—Description of the group.

group-id—Identifier for this group VPN. Specify a value from 1 to 65,535.

ike-gateway—Define the group member for Phase 1 negotiation. There can be multiple instances of this option configured, one for each member of the group. When a group member sends its registration request to the server, the server checks to see that the member is configured for the group.

ipsec-sa ***name***—Define the group SAs to be downloaded to members. There can be multiple group SAs downloaded to group members. A group SA definition consists of the following:

- **proposal** ***name***—Specify the name of the IPsec proposal configured with the **proposal** configuration statement at the [**edit security group-vpn server ipsec**] hierarchy.
- **match-policy** ***name***—Configure the group policy with source address, source port, destination address, destination port, and protocol.

  Use **0.0.0.0** to specify any source or destination. Use **0** to specify any source port, destination port, or protocol.

no-anti-replay—Disable the antireplay mechanism.

server-address—(Required) IP address of the group server.

NOTE: We recommend that you use the loopback address of the device for server-address.

server-member-communication—Enable and configure server to member communication. When these options are configured, group members receive new keys before current keys expire. These options also enable members to receive heartbeat messages from the server; members can detect server reboots when heartbeats are missed.

The following options can be configured for **server-member-communication**:

Copyright © 2011, Juniper Networks, Inc.

- **certificate**—Specify the certificate identification. Only RSA keys are supported.
- **communications-type**—Configure unicast (the default) or multicast. If multicast is specified, you need to specify an IPv4 multicast address for the **multicast-group** option.
- **encryption-algorithm**—Encryption used for communications between the group server and group member. Specify 3des-cbc, aes-128-cbc, aes-192-cbc, aes-256-cbc, or des-cbc.
- **heartbeat**— Interval, in seconds, at which the group server sends heartbeats to the group member. Specify a value from 60 to 3600. The default is 300 seconds.
- **lifetime-seconds**—Lifetime, in seconds, for the key encryption key (KEK). Specify a value from 180 to 86,400. The default is 3600 seconds.
- **multicast-group**—If **communications-type** is multicast, specify the multicast address for the group.
- **multicast-outgoing-interface**—If **communications-type** is multicast, specify the name of the interface on which multicast packets are sent.
- **number-of-retransmission**—For unicast communications, the number of times the group server retransmits messages to a group member when there is no reply. For multicast communications, the number of copies of a message the group server sends to group members. Specify a value from 0 to 60. The default is 2.
- **retransmission-period**—The time period between a transmission and the first retransmission when there is no reply from the group member. Specify a value from 2 to 60. The default is 4 seconds.
- **sig-hash-algorithm**—Authentication algorithm used to authenticate the group member to the group server. Specify md5 or sha1.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

group-members

Syntax group-members [attack-group-name | attack-name];

Hierarchy Level [edit security idp custom-attack-group *custom-attack-group-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the group members in a custom group. The members can be predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups.

Use custom groups for the following tasks:

- To define a specific set of attacks to which you know your network is vulnerable.
- To group your custom attack objects.
- To define a specific set of informational attack objects that you use to keep you aware of what is happening on your network.

Options **attack-group-name**—Name of the group attack object.

attack-name—Name of the attack object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

group-vpn

Syntax

```
group-vpn {
  co-location;
  member {
    ike {
      gateway gateway-name {
        address [(ip-address | hostname)];
        ike-policy policy-name;
        local-address address;
        local-identity (distinguished-name string | hostname hostname | inet ipv4-ip-address
          | user-at-hostname e-mail-address);
      }
      policy name {
        certificate {
          local-certificate identifier;
          peer-certificate-type [pkcs7 | x509-signature);
          trusted-ca (ca-index | use-all);
        }
        description text;
        mode (aggressive | main);
        pre-shared-key (ascii-text text | hexadecimal hex);
        proposal-set (basic | compatible | standard);
        proposals name;
      }
      proposal name {
        authentication-algorithm (md5 | sha-256 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description text;
        dh-group (group1 | group2 | group5 | group14);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
      }
    }
    ipsec vpn name {
      group id;
      group-vpn-external-interface interface;
      heartbeat-threshold number;
      ike-gateway name;
    }
  }
  server {
    group name{
      activation-time-delay seconds;
      anti-replay-time-window seconds;
      description text;
      group-id number;
      ike-gateway gateway-name;
      ipsec-sa name {
        proposal name;
          match-policy name {
            destination ip-address/netmask;
            destination-port number;
            protocol number;
```

```
            source ip-address/netmask;
            source-port number;
        }
    }
    no-anti-replay;
    server-address ip-address;
    server-member-communication {
        certificate certificate-id;
        communication-type (multicast | unicast);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        heartbeat seconds;
        lifetime-seconds seconds;
        multicast-group address;
        multicast-outgoing-interface interface;
        number-of-retransmission number;
        retransmission-period seconds;
        sig-hash-algorithm (md5 | sha1);
    }
}
ike {
    gateway name {
        address ( ip-address | hostname );
        dynamic {
            distinguished-name {
                container string;
                wildcard string;
            }
            hostname name;
            inet ip-address;
            user-at-hostname email-address;
        }
        ike-policy name;
        local-identity {
            distinguished-name;
            hostname name;
            inet ip-address;
            user-at-hostname emailaddress;
        }
    }
    policy name {
        certificate {
            local-certificate identifier;
            peer-certificate-type [pkcs7 | x509-signature);
            trusted-ca (ca-index | use-all);
        }
        description text;
        mode (aggressive | main);
        pre-shared-key (ascii-text text | hexadecimal hex);
        proposal-set (basic | compatible | standard);
        proposals name;
    }
    proposal name {
        authentication-algorithm (md5 | sha-256 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description text;
        dh-group (group1 | group2 | group5 | group14);
```


Copyright © 2011, Juniper Networks, Inc.

```
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
            lifetime-seconds seconds;
          }
        }
        ipsec proposal name {
          authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
          description text;
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
          lifetime-seconds seconds;
        }
        traceoptions {
          file {
            files number;
            match regexp;
            (no-world-readable | world-readable);
            size size;
          }
          flag {
            all | certificates | config | database | general | high-availability | ike
            | next-hop-tunnels | parse | policy-manager | routing-socket | thread | timer
          }
          no-remote-trace;
        }
      }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure group VPNs.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

gtp

Syntax

```
gtp {
  enable;
  profile profile name {
    apn pattern-string {
      mcc-mnc <mcc-mnc-number> {
        action <drop | pass | selection <ms | net | vrf> {
          }
        }
    drop {
    aa-create-pdp {
      <0 | 1 | All>;
    }
    aa-delete-pdp {
      <0 | 1 | All>;
    }
    create pdp {
      <0 | 1 | All>;
    }
    data-record {
      <0 | 1 | All>;
    }
    delete-pdp {
      <0 | 1 | All>;
    }
    echo {
      <0 | 1 | All>;
    }
    error-indication {
      <0 | 1 | All>;
    }
    failure-report {
      <0 | 1 | All>;
    }
    fwd-relocation {
      <0 | 1 | All>;
    }
    fwd-srns-context {
      <0 | 1 | All>;
    }
    g-pdu {
      <0 | 1 | All>;
    }
    identification {
      <0 | 1 | All>;
    }
    node-alive {
      <0 | 1 | All>;
    }
    note-ms-present {
      <0 | 1 | All>;
    }
    pdu-notification {
```


Copyright © 2011, Juniper Networks, Inc.

```
            <0 | 1 | All>;
          }
          ran-info {
            <0 | 1 | All>;
          }
          redirection {
            <0 | 1 | All>;
          }
          relocation-cancel {
            <0 | 1 | All>;
          }
          send-route {
            <0 | 1 | All>;
          }
          sgsn-context {
            <0 | 1 | All>;
          }
          supported-extension {
            <0 | 1 | All>;
          }
          update-pdp {
            <0 | 1 | All>;
          }
          ver-not-supported {
            <0 | 1 | All>;
          }
          log {
            forwarded <basic | detail>;
            prohibited <basic | detail>;
            rate-limited <basic | detail>;
              frequency-number <number>;
              }
            state-invalid <basic | detail>;
          }
          max-message-length number;
          min-message-length number;
          rate-limit messages per second;
          remove-r6;
          seq-number-validated;
          timeout <number of hours>;
          }
        }
        traceoptions
          file filename {
            <files | match | no-world-readable | size | world-readable>;
            }
          flag {
            < all | chassis-cluster | configuration | flow | parser | >;
            }
          no-remote-trace;
      }
    }
```

Hierarchy Level [edit security gprs]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Use the GTP commands to enable the GTP service, configure GTP objects, set traceoptions, remove GTP inspection-object configurations, and obtain configuration information.

A Juniper Networks security device provides firewall protection for the following types of GPRS interfaces:

- Gn—The Gn interface is the connection between an SGSN and a GGSN within the same Public Land Mobile Network (PLMN).
- Gp—The Gp interface is the connection between two Public Land Mobile Network PLMNs.
- Gi—The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

h323

Syntax

```
h323 {
  application-screen {
    message-flood {
      gatekeeper threshold rate ;
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  endpoint-registration-timeout seconds ;
  media-source-port-any;
  traceoptions {
    flag {
      all <detail | extensive | terse>;
      cc <detail | extensive | terse>;
      h225-asn1 <detail | extensive | terse>;
      h245 <detail | extensive | terse>;
      h245-asn1 <detail | extensive | terse>;
      q931 <detail | extensive | terse>;
      ras <detail | extensive | terse>;
      ras-asn1 <detail | extensive | terse>;
    }
  }
}
```

Hierarchy Level

[edit security alg]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the H.323 Application Layer Gateway (ALG) on the device. H.323 is a control-signaling protocol used to exchange messages between H.323 endpoints.

Options

disable—Disable the H.323 ALG. By default, H.323 ALG is enabled.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

handshake-timeout

Syntax handshake-timeout *time in seconds*;

Hierarchy Level [edit security gprs sctp profile *name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Set the handshake time for Stream Control Transmission Protocol (SCTP).

Options **seconds**—Number of seconds of handshake time that elapse before the session is terminated. **Range:** 1 to 30 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

header-length

Syntax

```
header-length {
   match (equal | greater-than | less-than | not-equal);
   value header-length;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the number of bytes in the TCP header.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***header-length*** —Match the number of bytes in the TCP header.
Range: 0 through 15 bytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

hit-rate-threshold

Syntax

```
context <context-name> {
   hit-rate-threshold number;
}
```

Hierarchy Level

[edit security idp application-ddos *name* context *context-name*]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure context hit rate thresholds to start bot client classifications for application-level distributed denial-of-service (DDoS) protection. The value is measured in number of contexts seen in tick interval (one tick is equal to 60 seconds). The context is an application protocol context such as: http-url and dns-cname. When the threshold is reached, the system will begin client classification using time-binding, if time-binding parameters are configured.

If time-binding is not configured, the system will skip bot client classification, and the configured policy actions are taken. This could result in valid clients being applied with configured policy actions. Time-binding configuration (count and period) should be used for bot client classification. However, this feature can be used as an Application Layer screen to deny resource access for all clients when context **hit-rate-threshold** is exceeded.

The context hit rate is the number of hits in tick interval for the same context type, for example: http-url for a specific application-level DDoS protected application.

Options

threshold *number* —Context hit rate threshold from bot client.

Range:

- SRX3400– 1 to 250,000,000
- SRX3600–1 to 500,000,000
- SRX5600/5800–1 to 2,500,000,000

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

high-watermark

Syntax high-watermark *percent* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Sets the point at which the aggressive aging-out process begins.

Options *percent* —Percentage of session-table capacity at which aggressive aging-out starts.
Range: 1 through 100 percent
Default: 100 percent

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

host

Syntax host *host-name*;

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Set server host parameters by entering the server name or IP address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

host (Security Logging)

Syntax host *ip-address*

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description You can specify the IP address of the server to which the security logs will be streamed.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

host (IDP Sensor Configuration)

Syntax host *ip-address* port *number*

Hierarchy Level [edit security idp sensor-configuration packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the IP address and port number of the server where the packet capture object will be sent.

Options host *ip-address*—The IP address of the server where the packet capture object will be sent.

port *number*—The port number of the server where the packet capture object will be sent.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

host-address-base

Syntax host-address-base *ip-address* ;

Hierarchy Level [edit security nat source pool *pool-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the base address of the original source IP address range. This is used for IP shifting.

Options *ip-address* —IP address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

host-inbound-traffic

Syntax

```
host-inbound-traffic {
  protocols {
    protocol-name ;
    protocol-name  <except>;
  }
  system-services {
    service-name ;
    service-name  <except>;
  }
}
```

Hierarchy Level [edit security zones functional-zone management],
[edit security zones functional-zone management interfaces *interface-name*],
[edit security zones security-zone *zone-name*],
[edit security zones security-zone *zone-name* interfaces *interface-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Control the type of traffic that can reach the device from interfaces bound to the zone.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

hostname

Syntax **hostname** ***domain-name*** **;**

Hierarchy Level [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description Unique name by which a network-attached device is known on a network.

Options ***domain-name*** —A fully qualified domain name (FQDN).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

http-profile (antivirus utm-policy)

Syntax http-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

http-profile (content-filtering utm-policy)

Syntax http-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

http-profile (web-filtering utm-policy)

Syntax http-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* web-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the web-filtering HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

icmp (Protocol Binding Custom Attack)

Syntax icmp;

Hierarchy Level [edit security idp custom-attack ***attack-name*** attack-type chain protocol-binding]
[edit security idp custom-attack ***attack-name*** attack-type signature protocol-binding]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the attack for specified ICMP.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

icmp (Security Screen)

Syntax

```
icmp {
   flood {
      threshold number ;
   }
   fragment;
   ip-sweep {
      threshold number;
   }
   large;
   ping-death;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure ICMP intrusion detection service (IDS) options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

icmp (Signature Attack)

Syntax

```
icmp {
  code {
    match (equal | greater-than | less-than | not-equal);
    value code-value ;
  }
  data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length ;
  }
  identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value ;
  }
  sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number ;
  }
  type {
    match (equal | greater-than | less-than | not-equal);
    value type-value ;
  }
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the ICMP header information for the signature attack.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

identification (ICMP Headers in Signature Attack)

Syntax

```
identification {
   match (equal | greater-than | less-than | not-equal);
   value identification-value;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a unique value used by the destination system to associate requests and replies.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value *identification-value* —Match a decimal value.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

identification (IP Headers in Signature Attack)

Syntax

```
identification {
   match (equal | greater-than | less-than | not-equal);
   value identification-value;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a unique value used by the destination system to reassemble a fragmented packet.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value *identification-value* —Match a decimal value.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

idle-time

Syntax idle-time *seconds* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum amount of idle time to delete a security association (SA).

Options *seconds* —Maximum amount of idle time.
Range: 60 through 999999 seconds
Default: To be disabled

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

idp

Syntax

```
idp {
  active-policy policy-name ;
  custom-attack attack-name {
    attack-type {
      anomaly {
        direction (any | client-to-server | server-to-client);
        service service-name ;
        shellcode (all | intel | no-shellcode | sparc);
        test test-condition ;
      }
      chain {
        expression boolean-expression ;
        member member-name {
          attack-type {
            (anomaly | signature);
          }
        }
        order;
        protocol-binding {
          application application-name ;
          icmp;
          ip {
            protocol-number transport-layer-protocol-number ;
          }
          rpc {
            program-number rpc-program-number ;
          }
          tcp {
            minimum-port port-number maximum-port port-number ;
          }
          udp {
            minimum-port port-number maximum-port port-number ;
          }
        }
        reset;
        scope (session | transaction);
      }
      signature {
        context context-name ;
        direction (any | client-to-server | server-to-client);
        negate;
        pattern signature-pattern ;
        protocol {
          icmp {
            code {
              match (equal | greater-than | less-than | not-equal);
              value code-value ;
            }
            data-length {
              match (equal | greater-than | less-than | not-equal);
              value data-length ;
            }
```

```
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value ;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number ;
    }
    type {
      match (equal | greater-than | less-than | not-equal);
      value type-value ;
    }
  }
  ip {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value hostname ;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value ;
    }
    ip-flags {
      (df | no-df);
      (mf | no-mf);
      (rb | no-rb);
    }
    protocol {
      match (equal | greater-than | less-than | not-equal);
      value transport-layer-protocol-id ;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value hostname ;
    }
    tos {
      match (equal | greater-than | less-than | not-equal);
      value type-of-service-in-decimal ;
    }
    total-length {
      match (equal | greater-than | less-than | not-equal);
      value total-length-of-ip-datagram ;
    }
    ttl {
      match (equal | greater-than | less-than | not-equal);
      value time-to-live ;
    }
  }
  tcp {
    ack-number {
      match (equal | greater-than | less-than | not-equal);
      value acknowledgement-number ;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value tcp-data-length ;
```

 Copyright © 2011, Juniper Networks, Inc.

```
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port ;
    }
    header-length {
      match (equal | greater-than | less-than | not-equal);
      value header-length ;
    }
    mss {
      match (equal | greater-than | less-than | not-equal);
      value maximum-segment-size ;
    }
    option {
      match (equal | greater-than | less-than | not-equal);
      value tcp-option ;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number ;
    }
    source-port {
      match (equal | greater-than | less-than | not-equal);
      value source-port ;
    }
    tcp-flags {
      (ack | no-ack);
      (fin | no-fin);
      (psh | no-psh);
      (r1 | no-r1);
      (r2 | no-r2);
      (rst | no-rst);
      (syn | no-syn);
      (urg | no-urg);
    }
    urgent-pointer {
      match (equal | greater-than | less-than | not-equal);
      value urgent-pointer ;
    }
    window-scale {
      match (equal | greater-than | less-than | not-equal);
      value window-scale-factor ;
    }
    window-size {
      match (equal | greater-than | less-than | not-equal);
      value window-size ;
    }
  }
  udp {
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length ;
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port ;
```

```
                }
                source-port {
                    match (equal | greater-than | less-than | not-equal);
                    value source-port ;
                }
            }
        }
        protocol-binding {
            application application-name ;
            icmp;
            ip {
                protocol-number transport-layer-protocol-number ;
            }
            rpc {
                program-number rpc-program-number ;
            }
            tcp {
                minimum-port port-number maximum-port port-number ;
            }
            udp {
                minimum-port port-number maximum-port port-number ;
            }
        }
        regexp regular-expression ;
        shellcode (all | intel | no-shellcode | sparc);
    }
}
recommended-action (close | close-client | close-server | drop |
drop-packet | ignore | none);
severity (critical | info | major | minor | warning);
time-binding {
    count count-value ;
    scope (destination | peer | source);
}
}
custom-attack-group custom-attack-group-name {
    group-members [attack-group-name | attack-name];
}
dynamic-attack-group dynamic-attack-group-name {
    filters {
        category {
            values [list-of-values];
        }
        direction {
            values [any | client-to-server | exclude-any | exclude-client-to-server |
            exclude-server-to-client | server-to-client];
        }
        false-positives {
            values [frequently | occasionally | rarely | unknown];
        }
        performance {
            values [fast | normal | slow | unknown];
        }
        products {
            values [list-of-values];
        }
```


Copyright © 2011, Juniper Networks, Inc.

```
        recommended;
        service {
          values [list-of-values];
        }
        severity {
          values [critical | info | major | minor | warning];
        }
        type {
          values [anomaly | signature];
        }
      }
    }
    idp-policy policy-name {
      rulebase-exempt {
        rule rule-name {
          description text ;
          match {
            application [ application-name ];
            attacks {
              custom-attacks [ attack-name ];
              predefined-attack-groups [ attack-name ];
              predefined-attacks [ attack-name ];
            }
            destination-address [ address-name ];
            destination-except [ address-name ];
            from-zone zone-name ;
            source-address [ address-name ];
            source-except [ address-name ];
            to-zone zone-name ;
          }
        }
      }
      rulebase-ips {
        rule rule-name {
          description text ;
          match {
            attacks {
              custom-attacks [ attack-name ];
              predefined-attack-groups [ attack-name ];
              predefined-attacks [ attack-name ];
            }
            destination-address [ address-name ];
            destination-except [ address-name ];
            from-zone zone-name ;
            source-address [ address-name ];
            source-except [ address-name ];
            to-zone zone-name ;
          }
          terminal;
          then {
            action {
              (close-client | close-client-and-server | close-server |
              drop-connection | drop-packet | ignore-connection |
              mark-diffserv value | no-action | recommended);
            }
            ip-action {
```

```
                (ip-block | ip-close | ip-notify);
                log;
                target (destination-address | service | source-address |
                source-zone | zone-service);
                timeout seconds;
            }
            notification {
                log-attacks {
                    alert;(
                }
            }
            severity (critical | info | major | minor | warning);
        }
    }
  }
}
security-package {
  automatic {
    enable;
    interval hours ;
    start-time start-time ;
  }
  url url-name ;
}
sensor-configuration {
  application-identification {
    application-system-cache;
    application-system-cache-timeout value ;
    disable;
    max-packet-memory value ;
    max-sessions value ;
    max-tcp-session-packet-memory value ;
    max-udp-session-packet-memory value ;
    nested-application-system-cache;
    nested-application;
  }
  detector {
    protocol-name protocol-name {
      tunable-name tunable-name {
        tunable-value protocol-value ;
      }
    }
  }
  flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    (log-errors | no-log-errors);
    max-timers-poll-ticks value ;
    reject-timeout value ;
    (reset-on-policy | no-reset-on-policy);
  }
  global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    (policy-lookup-cache | no-policy-lookup-cache);
  }
  ips {
```

 Copyright © 2011, Juniper Networks, Inc.

```
        detect-shellcode;
        ignore-regular-expression;
        log-supercede-min minimum-value ;
        pre-filter-shellcode;
        process-ignore-s2c;
        process-override;
        process-port port-number ;
      }
      log {
        cache-size size ;
        suppression {
          disable;
          include-destination-address;
          max-logs-operate value ;
          max-time-report value ;
          start-log value ;
        }
      }
      re-assembler {
        ignore-mem-overflow;
        max-flow-mem value ;
        max-packet-mem value ;
      }
    }
    traceoptions {
      file filename {
        <files number >;
        <match regular-expression >;
        <size maximum-file-size >;
        <world-readable | no-world-readable>;
      }
      flag all;
      level (all | error | info | notice | verbose | warning);
      no-remote-trace;
    }
  }
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 9.3 of Junos OS.

Description Configure Intrusion Detection and Prevention (IDP) to selectively enforce various IDP attack detection and prevention techniques on the network.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

idp-policy

Syntax

```
idp-policy policy-name {
  rulebase-exempt {
    rule rule-name {
      description text ;
      match {
        application [ application-name ];
        attacks {
          custom-attacks [ attack-name ];
          predefined-attack-groups [ attack-name ];
          predefined-attacks [ attack-name ];
        }
        destination-address [ address-name ];
        destination-except [ address-name ];
        from-zone zone-name ;
        source-address [ address-name ];
        source-except [ address-name ];
        to-zone zone-name ;
      }
    }
  }
  rulebase-ips {
    rule rule-name {
      description text ;
      match {
        attacks {
          custom-attacks [ attack-name ];
          predefined-attack-groups [ attack-name ];
          predefined-attacks [ attack-name ];
        }
        destination-address [ address-name ];
        destination-except [ address-name ];
        from-zone zone-name ;
        source-address [ address-name ];
        source-except [ address-name ];
        to-zone zone-name ;
      }
      terminal;
      then {
        action {
          (close-client | close-client-and-server | close-server |
          drop-connection | drop-packet | ignore-connection |
          mark-diffserv value | no-action | recommended);
        }
        ip-action {
          (ip-block | ip-close | ip-notify);
          log;
          target (destination-address | service | source-address |
          source-zone | zone-service);
          timeout seconds;
        }
        notification {
          log-attacks {
```


Copyright © 2011, Juniper Networks, Inc.

```
                alert;(
            }
            packet-log {
                pre-attack number;
                post-attack number;
                post-attack-timeout seconds;
            }
        }
        severity (critical | info | major | minor | warning);
    }
  }
}
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure a security IDP policy.

Options ***policy-name*** —Name of the IDP policy.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ids-option

Syntax

```
ids-option screen-name {
  alarm-without-drop;
  icmp {
    flood {
      threshold number ;
    }
    fragment;
    ip-sweep {
      threshold number ;
    }
    large;
    ping-death;
  }
  ip {
    bad-option;
    block-frag;
    loose-source-route-option;
    record-route-option;
    security-option;
    source-route-option;
    spoofing;
    stream-option;
    strict-source-route-option;
    tear-drop;
    timestamp-option;
    unknown-protocol;
  }
  limit-session {
    destination-ip-based number ;
    source-ip-based number ;
  }
  tcp {
    fin-no-ack;
    land;
    port-scan {
      threshold number ;
    }
    syn-ack-ack-proxy {
      threshold number ;
    }
    syn-fin;
    syn-flood {
      alarm-threshold number ;
      attack-threshold number ;
      destination-threshold number ;
      source-threshold number ;
      timeout seconds ;
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
      threshold threshold number;
```


Copyright © 2011, Juniper Networks, Inc.

```
            }
            winnuke;
        }
        udp {
            flood {
                threshold number ;
            }
            udp-sweep {
                threshold threshold number;
            }
        }
    }
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define screens for intrusion detection and prevention.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ignore-mem-overflow

Syntax ignore-mem-overflow;

Hierarchy Level [edit security idp sensor-configuration re-assembler]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable the TCP reassembler to ignore the memory overflow to prevent the dropping of IDP custom applications. By default this feature is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ignore-regular-expression

Syntax ignore-regular-expression;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable regular expression to detect intrusion attempts. By default this setting is disabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ike (Group VPN Member)

Syntax

```
ike {
  gateway gateway-name {
    address [(ip-address | hostname)];
    ike-policy policy-name;
    local-address address;
    local-identity (distinguished-name string | hostname hostname | inet ipv4-ip-address |
      user-at-hostname e-mail-address);
  }
  policy name {
    certificate {
      local-certificate identifier;
      peer-certificate-type [pkcs7 | x509-signature);
      trusted-ca (ca-index | use-all);
    }
    description text;
    mode (aggressive | main);
    pre-shared-key (ascii-text text | hexadecimal hex);
    proposal-set (basic | compatible | standard);
    proposals name;
  }
  proposal name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description text;
    dh-group (group1 | group2 | group5 | group 14);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
  }
}
```

Hierarchy Level [edit security group-vpn member]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure IPsec group VPN on the group member.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ike (Group VPN Server)

Syntax

```
ike {
  gateway name {
    address ( ip-address | hostname );
    dynamic {
      distinguished-name {
        container string;
        wildcard string;
      }
      hostname name;
      inet ip-address;
      user-at-hostname email-address;
    }
    ike-policy name;
    local-identity {
      distinguished-name;
      hostname name;
      inet ip-address;
      user-at-hostname emailaddress;
    }
  }
  policy name {
    certificate {
      local-certificate identifier;
      peer-certificate-type [pkcs7 | x509-signature);
      trusted-ca (ca-index | use-all);
    }
    description text;
    mode (aggressive | main);
    pre-shared-key (ascii-text text | hexadecimal hex);
    proposal-set (basic | compatible | standard);
    proposals name;
  }
  proposal name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description text;
    dh-group (group1 | group2 | group5 | group 14);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
  }
}
```

Hierarchy Level [edit security group-vpn server]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure Phase 1 security association (SA) with a member on the group server. The gateway is the group member.

Options The remaining statements are explained separately.

 Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ike (IPsec VPN)

Syntax

```
ike {
   gateway gateway -name ;
   idle-time seconds ;
   install-interval seconds ;
   ipsec-policy ipsec-policy-name ;
   no-anti-replay;
   proxy-identity {
      local ip-prefix ;
      remote ip-prefix ;
      service service-name ;
   }
}
```

Hierarchy Level
[edit security ipsec vpn *vpn-name*]

Release Information
Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description
Define an IKE-keyed IPsec VPN.

Options
The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ike (Security)

Syntax

```
ike {
  gateway gateway-name {
    address [( ip-address | hostname )] |
    dead-peer-detection {
      always-send;
      interval seconds ;
      threshold number ;
    }
    dynamic {
      connections-limit number ;
      distinguished-name {
        container container-string ;
        wildcard wildcard-string ;
      }
      hostname domain-name ;
      ike-user-type (group-ike-id | shared-ike-id);
      inet ip-address ;
      inet6 ipv6-address ;
      user-at-hostname user-at-hostname ;
    }
    external-interface external-interface-name ;
    ike-policy policy-name ;
    local-identity (hostname hostname | inet ip-address | inet6 ipv6-address |
    user-at-hostname e-mail-address | distinguished-name string );
    nat-keepalive seconds ;
    no-nat-traversal;
    xauth {
      access-profile profile-name ;
    }
  }
  policy policy-name {
    certificate {
      local-certificate certificate-id ;
      peer-certificate-type (pkcs7 | x509-signature);
      trusted-ca ( ca-index | use-all);
    }
    description description ;
    mode (aggressive | main);
    pre-shared-key (ascii-text | hexadecimal);
    proposal-set (basic | compatible | standard);
    proposals [proposal-names];
  }
  proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description ;
    dh-group (group1 | group2 | group5 | group14);
    encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
    | aes-256-cbc);
    lifetime-seconds seconds ;
  }
  respond-bad-spi number ;
```


Copyright © 2011, Juniper Networks, Inc.

```
  traceoptions {
    file {
      files number ;
      size maximum-file-size ;
    }
    flag {
      all;
      certificates;
      database;
      general;
      ike;
      parse;
      policy-manager;
      routing-socket;
      timer;
      snmp;
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS.

Description Define Internet Key Exchange (IKE) configuration.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ike-policy

Syntax ike-policy *policy-name* ;

Hierarchy Level [edit security group-vpn member ike gateway *gateway-name*]
[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify the IKE policy to be used for the gateway.

Options *policy-name* —IKE policy name.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ike-user-type

Syntax **ike-user-type (group-ike-id | shared-ike-id);**

Hierarchy Level **[edit security ike gateway *gateway-name* dynamic]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the type of IKE user for a remote access connection.

Options **group-ike-id**—E-mail address or fully qualified domain name (FQDN) shared for a group of remote access users so that each one does not need a separate IKE profile configured.

shared-ike-id—E-mail address shared for a large number of remote access users so that each one does not need a separate IKE profile configured.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

imap-profile (antivirus utm-policy)

Syntax imap-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

imap-profile (content-filtering utm-policy)

Syntax imap-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inactive-media-timeout (MGCP)

Syntax inactive-media-timeout *seconds* ;

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

Options ***seconds*** —Maximum amount of time that the pinholes remain open.

Range: 10 through 2550 seconds

Default: 120 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inactive-media-timeout (SCCP)

Syntax inactive-media-timeout *seconds* ;

Hierarchy Level [edit security alg sccp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

Options ***seconds*** —Maximum amount of time that the pinholes remain open.

Range: 10 through 600 seconds

Default: 120 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

inactive-media-timeout (SIP)

Syntax inactive-media-timeout *seconds* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

Options ***seconds*** —Maximum amount of time that the pinholes remain open.

Range: 0 through 2550 seconds

Default: 120 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inactivity-timeout

Syntax inactivity-timeout *seconds*;

Hierarchy Level [edit security nat source rule-set *ruleset* rule *rule* then source-nat (pool | interface) persistent-nat]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description The amount of time, in seconds, that the persistent NAT binding remains in the Juniper Networks device's memory when all the sessions of the binding entry are gone. When the configured timeout is reached, the binding is removed from memory.

Options *seconds*—Number of seconds.

Range: 60 through 7200 seconds

Default: 300 seconds (5 minutes)

Required Privilege Level **security**—To view this statement in the configuration.
security-control—To add this statement to the configuration

Related Documentation
- *Junos OS Security Configuration Guide*

include-destination-address

Syntax include-destination-address;

Hierarchy Level [edit security idp sensor-configuration log suppression]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description When log suppression is enabled, multiple occurrences of events with the same source, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression will only combine log records for events with a matching source as well. The IDP Sensor does not consider destination when determining matching events for log suppression. By default this setting is disabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inet

Syntax inet *ip-address* ;

Hierarchy Level [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description Specify IP address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

Options *ip-address* —IP address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

inet6

Syntax

```
inet6 {
   mode (packet-based | flow-based | drop ); default: drop
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable packet-based or flow-based processing of IPv6 traffic. By default, the device drops IPv6 traffic.

Options The **mode** statement is described separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

inet6 (IKE Gateway)

Syntax **inet6** ***ipv6-address*****;**

Hierarchy Level **[edit security ike gateway** ***gateway-name*** **dynamic]**

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Specify an IPv6 address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

Options ***ipv6-address*** —IPv6 address.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

inline-tap

Syntax inline-tap;

Hierarchy Level [edit security forwarding-process application-services maximize-idp-sessions]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Enable IDP inline tap mode. The inline tap feature provides passive, inline detection of application layer threats for traffic matching security policies which have the IDP application service enabled. When a device is in inline tap mode, packets pass through firewall inspection and are also copied to the independent IDP module.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

install-interval

Syntax install-interval *seconds* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device.

Options *seconds* —Maximum amount of idle time.

Range: 0 through 10 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

intelligent-prescreening

Syntax intelligent-prescreening;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* scan-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

Options
- intelligent-prescreening—Turns the feature on.
- no-intelligent-prescreening—Turns the feature off.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

interface (ARP Proxy)

Syntax
```
interface interface-name {
  address ip-address to ip-address ;
}
```

Hierarchy Level [edit security nat proxy-arp]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the interface on which the ARP proxy is to be configured. It should be a logical interface.

Options *interface-name* —Name of the logical interface.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

interface (Source NAT)

Syntax

```
interface {
  persistent-nat {
    address-mapping;
    inactivity-timeout seconds;
    max-session-number number;
    permit ( any-remote-host | target-host | target-host-port );
  }
  port-overloading { off };
}
```

Hierarchy Level [edit security nat source]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Enable interface NAT with or without port overloading.

Options **port-overloading**—Specify **off** when persistent NAT is configured for interface NAT.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

interfaces

Syntax

```
interfaces interface-name {
  host-inbound-traffic {
    protocols {
      protocol-name ;
      protocol-name <except>;
    }
    system-services {
      service-name ;
      service-name <except>;
    }
  }
}
```

Hierarchy Level [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the set of interfaces that are part of the zone.

Options *interface-name* —Name of the interface.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

interval (IDP)

Syntax interval *hours* ;

Hierarchy Level [edit security idp security-package automatic]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the amount of time that the device waits before updating the signature database. User should insert a default value.

Options *hours* —Number of hours that the device waits.

Range: 24 through 336 hours

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

interval (IKE)

Syntax interval *seconds* ;

Hierarchy Level [edit security ike gateway *gateway-name* dead-peer-detection]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet.

Options ***seconds*** —Number of seconds that the peer waits before sending a DPD request packet.

Range: 0 through 60 seconds

Default: 10 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

interval (kaspersky-lab-engine)

Syntax interval *value*;

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description The default pattern-update interval value is 60 minutes. You can choose to leave this default as is or you can change it using this command. You can also force a manual update, if necessary.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

interval (juniper-express-engine)

Syntax interval *value*;

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description The default pattern-update interval value is 60 minutes. You can choose to leave this default as is or you can change it by using this command. You can also force a manual update, if necessary.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

interval (sophons-engine)

Syntax interval *value*;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine pattern-update]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description The default pattern update interval for Sophos antivirus is 1440 minutes (every 24 hours). You can choose to leave this default as is or you can change it by using this command. You can also force a manual update, if necessary.

NOTE: The data files used with Sophos are not a typical virus pattern files, they are small file that helps guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

Options *value* —Pattern data files auto-update interval in minutes.

Range: 10 through 10,080 minutes (10 minutes through 7 days)

Default: 1440 minutes (every 24 hours)

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

ip (Protocol Binding Custom Attack)

Syntax

```
ip {
   protocol-number transport-layer-protocol-number;
}
```

Hierarchy Level

[edit security idp custom-attack ***attack-name*** attack-type chain protocol-binding]
[edit security idp custom-attack ***attack-name*** attack-type signature protocol-binding]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Allow IDP to match the attack for a specified IP protocol type.

Options

protocol-number ***transport-layer-protocol-number*** —Transport Layer protocol number.

Range: 0 through 139

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ip (Security Screen)

Syntax

```
ip {
   bad-option;
   block-frag;
   loose-source-route-option;
   record-route-option;
   security-option;
   source-route-option;
   spoofing;
   stream-option;
   strict-source-route-option;
   tear-drop;
   timestamp-option;
   unknown-protocol;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure IP layer IDS options.

Options

- **bad-option**—Detect and drop any packet with an incorrectly formatted IP option in the IP packet header. The device records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **block-frag**—Enable IP packet fragmentation blocking.
- **loose-source-route-option**—Detect packets where the IP option is 3 (loose source routing), and record the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified. The type 0 routing header of the loose source route option is the only related header defined in IPv6 .
- **record-route-option**—Detect packets where the IP option is 7 (record route), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **security-option**—Detect packets where the IP option is 2 (security), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **source-route-option**—Detect packets, and record the event in the screen counters list for the ingress interface.
- **spoofing**—Prevent spoofing attacks. Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Using the spoofing option invalidates such false source IP address connections.

  The default behavior is to base spoofing decisions on individual interfaces.

Copyright © 2011, Juniper Networks, Inc.

- **stream-option**—Detect packets where the IP option is 8 (stream ID), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **strict-source-route-option**—Detect packets where the IP option is 9 (strict source routing), and record the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable only to IPv4.
- **tear-drop**—Block the teardrop attack. Teardrop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. The teardrop option directs the device to drop any packets that have such a discrepancy.
- **timestamp-option**—Detect packets where the IP option list includes option 4 (Internet timestamp), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **unknown-protocol**—Discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. Such protocol numbers are undefined or reserved.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ip (Signature Attack)

Syntax

```
ip {
  destination {
    match (equal | greater-than | less-than | not-equal);
    value hostname ;
  }
  identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value ;
  }
  ip-flags {
    (df | no-df);
    (mf | no-mf);
    (rb | no-rb);
  }
  protocol {
    match (equal | greater-than | less-than | not-equal);
    value transport-layer-protocol-id ;
  }
  source {
    match (equal | greater-than | less-than | not-equal);
    value hostname ;
  }
  tos {
    match (equal | greater-than | less-than | not-equal);
    value type-of-service-in-decimal ;
  }
  total-length {
    match (equal | greater-than | less-than | not-equal);
    value total-length-of-ip-datagram ;
  }
  ttl {
    match (equal | greater-than | less-than | not-equal);
    value time-to-live ;
  }
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the IP header information for the signature attack.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-action

Syntax

```
ip-action {
   (ip-block | ip-close | ip-notify);
   log;
   target (destination-address | service | source-address |
   source-zone | zone-service);
   timeout seconds;
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the actions you want IDP to take against future connections that use the same IP address.

Options The remaining statements are explained separately.

NOTE: For ICMP flows, the destination port is 0; therefore, any ICMP flow matching source port, source address, and destination address is blocked.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ip-action (Application-Level DDoS)

Syntax

```
ip-action {
   [ip-block | ip-close | ip-notify];
   timeout seconds;
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Specify the actions you want IDP to take against future connections that use the same IP address.

Options

- **ip-block**—Block future connections of any session that matches the IP action.
- **ip-close**—Close future connections of any new sessions that match the IP action by sending RST packets to the client and server.
- **ip-notify**—Do not take any action against traffic, but do log the event.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-block

Syntax ip-block;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Block future connections of any session that matches the IP action. If there is an IP action match with multiple rules, then the most severe IP action of all the matched rules is applied. The highest IP action priority (that is, the most severe action) is Drop/Block, then Close, then Notify.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-close

Syntax ip-close;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Close future connections of any new sessions that match the IP action by sending RST packets to the client and server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ip-connection--rate-limit

Syntax ip-connection-rate-limit *value*;

Hierarchy Level [edit security idp idp-polciy *policy-name* rulebase-ddos rule *rule-name* then ip-action]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description When a match is made in a rulebase-ddos rule you can set the **then** action to ip-connection-rate-limit, which will rate limit future connections based on a connections per second limit that you set. This can be used to reduce the number of attacks from a client.

Options ***value*** —Defines the connection rate limit per second on the matched host.

Range: 1 to the maximum connections per second capability of the device.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

ip-flags

Syntax

```
ip-flags {
   (df | no-df);
   (mf | no-mf);
   (rb | no-rb);
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify that IDP looks for a pattern match whether or not the IP flag is set.

Options

df | no-df—When set, the df (Don't Fragment) indicates that the packet cannot be fragmented for transmission. When unset, it indicates that the packet can be fragmented.

mf | no-mf—When set, the mf (More Fragments) indicates that the packet contains more fragments. When unset, it indicates that no more fragments remain.

rb | no-rb—When set, the rb (Reserved Bit) indicates that the bit is reserved.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ip-notify

Syntax ip-notify;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Do not take any action against future traffic, but do log the event. This is the default.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ips

Syntax

```
ips {
   detect-shellcode;
   ignore-regular-expression;
   log-supercede-min minimum-value ;
   pre-filter-shellcode;
   process-ignore-s2c;
   process-override;
   process-port port-number ;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure IPS security policy sensor settings.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

ipsec (Group VPN Server)

Syntax

```
ipsec proposal name {
   authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
   description text;
   encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
   lifetime-seconds seconds;
}
```

Hierarchy Level

[edit security group-vpn server]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Configure IPsec proposal for Phase 2 exchange on the group server.

Options

proposal—Name of the proposal. The proposal name can be up to 32 alphanumeric characters long.

authentication-algorithm—Hash algorithm that authenticates packet data. It must be one of three algorithms:

- md5—Produces a 128-bit digest.
- sha-256—Produces a 256-bit digest.
- sha1—Produces a 160-bit digest.

description—Specify descriptive text for the IPsec proposal.

encryption-algorithm—Configure an IKE encryption algorithm. It must be one of the following:

- 3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long.
- des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.
- aes-128-cbc—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- aes-192-cbc—AES 192-bit encryption algorithm.
- aes-256-cbc—AES 256-bit encryption algorithm.

lifetime-seconds—Lifetime, in seconds, for this proposal. Specify a value from 180 to 86,400. The default is 3600 seconds.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ipsec-group-vpn (Group VPN)

Syntax ipsec-group-vpn *group-vpn*;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify group VPN tunnel for the traffic configured by the scope policy on a group member.

Options *group-vpn* —Name of the group VPN tunnel configured on the group member.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ipsec-policy

Syntax ipsec-policy *ipsec-policy-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the IPsec policy name.

Options *ipsec-policy-name* —Name of the IPsec policy.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

ipsec-vpn (Flow)

Syntax

```
ipsec-vpn {
  mss value ;
}
```

Hierarchy Level [edit security flow tcp-mss]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the TCP maximum segment size (TCP MSS) for the TCP packets that are about to go into an IPsec VPN tunnel. This value overrides the value specified in the **all-tcp-mss** statement.

Options

mss *value* —TCP MSS value for TCP packets entering an IPsec VPN tunnel. Value is optional.

Range: 64 through 65,535 bytes

Default: 1320 bytes

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ipsec-vpn (Policies)

Syntax ipsec-vpn *vpn-name* ;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define IPsec name for VPN.

Options *vpn-name* —Name of the IPsec.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ipsec-vpn (Dynamic VPNs)

Syntax ipsec-vpn *configuration-name*;

Hierarchy Level [edit security dynamic-vpn clients *configuration-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to specify which IPsec VPN configuration the dynamic VPN feature should use to secure traffic.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ip-sweep

Syntax

```
ip-sweep {
   threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and prevent an IP Sweep attack. An IP Sweep attack occurs when an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, it flags this as an IP Sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of the second.

Options **threshold *number***—Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the router. More than 10 requests from a host during this period triggers an IP Sweep attack response on the router during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

iso

Syntax

```
iso {
   mode packet-based;
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the forwarding of IS-IS traffic. By default, the device drops IS-IS traffic.

NOTE: Junos OS security processing is not applied to IS-IS packets forwarded by the device.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

juniper-express-engine

Syntax

```
juniper-express-engine {
pattern-update {
  email-notify {
    admin-email
      custom-message
    custom-message-subject
    }
    interval value;
    no-autoupdate
    url;
  }
  profile profile-name {
  fallback-options {
    default (log-and-permit | block);
      content-size (log-and-permit | block);
      engine-not-ready (log-and-permit | block);
      timeout (log-and-permit | block);
      out-of-resources (log-and-permit | block);
      too-many-requests (log-and-permit | block);
    }
    scan-options {
    intelligent-prescreening;
      scan-mode (scan-all | by--extension);
      content-size-limit value;
      timeout value;
      decompress-layer-limit value;
    }
    notification-options {
    virus-detection {
      type (message | protocol-only);
        notify-mail-sender;
        custom-message;
        custom-message-subject;
      }
      fallback-block {
      custom-message;
        custom-message-subject;
        notify-mail-sender;
        type;
      }
    }
    trickling {
      timeout value;
    }
  }
  mime-whitelist {
  list listname {
    exception listname;
  }
  url-whitelist {
  listname;
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the UTM express antivirus feature.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

juniper-local

Syntax

```
juniper-local {
  profile profile-name{
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      timeout;
      too-many-requests (block | log-and-permit);
    }
    timeout
}
```

Hierarchy Level [set security utm feature-profile web-filtering]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the UTM web-filtering local feature.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

kaspersky-lab-engine

Syntax

```
kaspersky-lab-engine {
pattern-update {
    email-notify {
      admin-email
        custom-message
      custom-message-subject
    }
  interval value;
    no-autoupdate;
    url;
  }
  profile profile-name {
  fallback-options {
    default (log-and-permit | block);
      corrupt-file (log-and-permit | block);
      password-file (log-and-permit | block);
      decompress-layer (log-and-permit | block);
      content-size (log-and-permit | block);
      engine-not-ready (log-and-permit | block);
      timeout (log-and-permit | block);
      out-of-resources (log-and-permit | block);
      too-many-requests (log-and-permit | block);
    }
    scan-options {
    intelligent-prescreening;
      scan-mode (scan-all | by--extension);
      content-size-limit value;
      timeout value;
      decompress-layer-limit value;
    }
    notification-options {
    virus-detection {
      type (message | protocol-only);
        notify-mail-sender;
        custom-message;
        custom-message-subject;
      }
      fallback-block {
      custom-message;
        custom-message-subject;
        notify-mail-sender;
        type;
      }
    }
    trickling {
      timeout value;
    }
  }
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Copyright © 2011, Juniper Networks, Inc.

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the UTM full file-based antivirus feature.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

land

Syntax land;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable prevention of Land attacks by combining the SYN flood defense with IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP addresses. The attacker sends these packets with the SYN flag set to any available port. The packets induce the target to create empty sessions with itself, filling its session table and overwhelming its resources.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

large

Syntax large;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and drop any ICMP frame with an IP length greater than 1024 bytes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

lifetime-kilobytes

Syntax lifetime-kilobytes ***kilobytes*** ;

Hierarchy Level [edit security ipsec proposal ***proposal-name***]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the lifetime (in kilobytes) of an IPsec security association (SA).

Options ***kilobytes*** —Lifetime of the IPsec security association (SA).

Range: 64 through 1048576 kilobytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

lifetime-seconds (Group VPN)

Syntax lifetime-seconds ***seconds*** ;

Hierarchy Level [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security group-vpn server ipsec proposal ***proposal-name***]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify the lifetime (in seconds) of an IKE or IPsec security association (SA) for group VPN. When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

Options ***seconds***—Lifetime of the IKE or IPsec SA.

Range: 180 through 86,400 seconds

Default: 3600 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

lifetime-seconds (IKE)

Syntax lifetime-seconds *seconds* ;

Hierarchy Level [edit security ike proposal *proposal-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Default value modified in Release 10.2.

Description Specify the lifetime (in seconds) of an IKE security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

Options *seconds*—Lifetime of the IKE SA.

Range: 180 through 86,400 seconds

Default: 28,800 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

lifetime-seconds (IPsec)

Syntax lifetime-seconds *seconds* ;

Hierarchy Level [edit security ipsec proposal *proposal-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Default value modified in Release 10.2.

Description Specify the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

Options *seconds*—Lifetime of the IPsec SA.

Range: 180 through 86,400 seconds

Default: 3600 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

limit

Syntax limit *value*;

Hierarchy Level [edit security utm utm-policy *policy-name* traffic-options sessions-per-client]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

limit (SCTP)

Syntax

```
limit {
  rate {
    address ip-address {
      sccp number;
      ssp number;
      sst number;
    }
    sccp number;
    ssp number;
    sst number;
  }
}
```

Hierarchy Level [edit security gprs sctp profile *name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Set the global messages rate limit. Four categories of global message rate limit can be set.

- **address**—To set Signalling Connection Control Part (SCCP), Subsystem-Prohibited (SSP), and Subsystem Status Test (SST) messages rate limit to an IP address.
- **sccp**—To set the SCCP messages rate limit.
- **ssp**—To set the SSP messages rate limit.
- **sst**—To set the SST messages rate limit.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

limit-session

Syntax

```
limit-session {
   destination-ip-based number ;
   source-ip-based number ;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the number of concurrent sessions the device can initiate from a single source IP address or the number of sessions it can direct to a single destination IP address.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

list (antivirus mime-whitelist)

Syntax

```
list listname {
exception listname;
```

Hierarchy Level [edit security utm feature-profile anti-virus mime-whitelist]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the antivirus scanner to use MIME bypass lists (custom objects).

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

list (content-filter block-mime)

Syntax

list *list-name* {
exception *list-name*;
}

Hierarchy Level

[edit security utm feature-profile content-filtering profile *profile-name* block-mime]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Configure the content filter to use MIME block lists (custom objects).

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

local

Syntax

local *ip-prefix*;

Hierarchy Level

[edit security ipsec vpn *vpn-name* ike proxy-identity]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description

Specify the local IPv4 or IPv6 address and subnet mask for the proxy identity.

Options

ip-prefix —IPv4 or IPv6 address and subnet mask.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

local-address

Syntax local–address *ip-address*;

Hierarchy Level [edit security group-vpn member ike gateway *gateway-name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the IP address the member uses when accessing the group server.

Options *ip-address*—IPv4 address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

local-certificate

Syntax local-certificate ***certificate-id*** ;

Hierarchy Level [edit security group-vpn member ike policy *policy-name* certificate]
[edit security group-vpn server ike policy *policy-name* certificate]
[edit security ike policy ***policy-name*** certificate]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify a particular certificate when the local device has multiple loaded certificates. (This statement is not supported on dynamic VPN implementations.)

Options ***certificate-id*** —Name of the specific certificate to be used.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

local-identity

Syntax

local-identity (distinguished-name *string* | hostname *hostname* | inet *ip-address* | inet6 *ipv6-address* | user-at-hostname *e-mail-address*);

Hierarchy Level

[edit security group-vpn member ike gateway *gateway-name*]
[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS. The **inet6** option is not supported on the **group-vpn** hierarchies.

Description

Specify the local IKE identity to send in the exchange with the destination peer so that the destination peer can communicate with the local peer. If you do not configure a local-identity, the device uses the IPv4 or IPv6 address corresponding to the local endpoint by default. (The **distinguished-name** option is not supported on dynamic VPN implementations.)

Options

distinguished-name ***string*** —Specify identity as the distinguished name (DN) from the certificate. If there is more than one certificate on the device, use the **security ike gateway** ***gateway-name*** **policy** ***policy-name*** **certificate local-certificate** ***certificate-id*** statement to specify a certificate.

hostname ***hostname***—Specify identity as a fully qualified domain name (FQDN).

inet ***ip-address***—Specify identity as an IPv4 address.

inet6 ***ipv6-address***—Specify identity as an IPv6 address.

user-at-hostname ***e-mail-address***—Specify identity as an e-mail address.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

log (GTP)

Syntax

```
log {
  forwarded <basic | detail>;
  prohibited <basic | detail>;
  rate-limited <basic | detail>;
    frequency-number <number>;
    }
  state-invalid <basic | detail>;
}
```

Hierarchy Level

[edit security gprs gtp profile *name*]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure GTP logs to be viewed from the console or syslog. Five categories of GTP packet logging can be set.

- **forwarded**—A packet that the security device transmitted because it was valid.
- **prohibited**—A packet that the security device dropped because it was invalid.
- **rate-limited**—A packet that the security device dropped because it exceeded the maximum rate limit of the destination GSN.
  - **frequency-number**—Logging frequency over threshold set by rate-limit (2–500)
- **state-invalid**—A packet that the security device dropped because it failed stateful inspection.

NOTE: All logs are disable by default.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

log (IDP)

Syntax

```
log {
  cache-size size ;
  suppression {
    disable;
    include-destination-address;
    max-logs-operate value ;
    max-time-report value ;
    start-log value ;
  }
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure IDP security policy logs.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

log (IDP Policy)

Syntax log;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Log the information about the IP action against the traffic that matches a rule.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

log (SCTP)

Syntax

```
log {
   configuration;
   decoding-error;
   dropped-packet;
   exceeding-rate-limit;
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure Stream Control Transmission Protocol (SCTP) logs to be viewed from the console or system log. Four categories of SCTP packet logging can be set.

- **configuration**—To log the CLI configuration.
- **decoding-error**—To log the decoding errors.
- **dropped-packet**—To log the dropped packets and out of resource errors.
- **exceeding-rate-limit**—To log the exceeding rate limit.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

log (Security Policies)

Syntax

```
log {
   session-close;
   session-init;
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable traffic to which the policy applies to be logged at the beginning or end of a session.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

log (Security Logging)

Syntax

```
log {
  mode (event | stream);
  event-rate rate;
  format (syslog | sd-syslog);
  stream stream-name format (syslog | sd-syslog | welf) category (all | content-security)
    host ip-address;
  traceoptions {
    file filename {
    files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | source);
  no-remote-trace;
}
```

Hierarchy Level

[edit security log]

Release Information

Statement introduced in Release 9.2 of Junos OS

Description

You can set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

log-attacks

Syntax

```
log-attacks {
   alert;
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable the log attacks to create a log record that appears in the log viewer.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

log-errors

Syntax (log-errors | no-log-errors);

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable the error log to generate the result of success or failure about the flow. A flow-related error is when IDP receives a packet that does not fit into expected flow. By default error log is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

log-supercede-min

Syntax log-supercede-min *minimum-value* ;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the amount of time to supersede the IPS sensor logs.

Options *minimum-value* —Minimum time to supersede the log.
Range: 0 through 65,535 seconds
Default: 1 second

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

low-watermark

Syntax low-watermark *percent* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Set the point at which the aggressive aging-out process ends.

Options *percent* —Percentage of session-table capacity at which aggressive aging-out ends.
Range: 0 through 100 percent
Default: 100 percent

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

management

Syntax

```
management {
  host-inbound-traffic {
    protocols {
      protocol-name ;
      protocol-name <except>;
    }
    system-services {
      service-name ;
      service-name <except>;
    }
  }
  interfaces interface-name {
    host-inbound-traffic {
      protocols {
        protocol-name ;
        protocol-name <except>;
      }
      system-services {
        service-name ;
        service-name <except>;
      }
    }
  }
  screen screen-name ;
}
```

Hierarchy Level

[edit security zones]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the host for out-of-band management interfaces. You can set firewall options in this zone to protect the management interface from different types of attacks. Because this zone cannot be specified in policies, traffic entering from this zone can only be traffic originating from the device itself and cannot transit out from any other zone.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

manual

Syntax

```
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key );
  }
  encryption {
    algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    key (ascii-text key | hexadecimal key );
  }
  external-interface external-interface-name ;
  gateway ip-address ;
  protocol (ah | esp);
  spi spi-value ;
}
```

Hierarchy Level

[edit security ipsec vpn *vpn-name*]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description

Define a manual IPsec security association (SA). (This statement is not supported on dynamic VPN implementations.)

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

match (Application Firewall)

Syntax

```
match {
  dynamic-application [dynamic-application-names];
}
```

Hierarchy Level [edit security application-firewall rule-sets *rule-set-name* rule *rule-name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Specify the application firewall rules to be used as match criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

match (Destination NAT)

Syntax

```
match {
  destination-address destination-address ;
  destination-port port-number ;
  source-address [source-address];
}
```

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the destination rules to be used as match criteria.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

match (IDP Policy)

Syntax

```
match {
  attacks {
    custom-attacks [ attack-name ];
    predefined-attack-groups [ attack-name ];
    predefined-attacks [ attack-name ];
  }
  destination-address [ address-name ];
  destination-except [ address-name ];
  from-zone zone-name ;
  source-address [ address-name ];
  source-except [ address-name ];
  to-zone zone-name ;
}
```

Hierarchy Level

[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name*],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

Release Information

Statement introduced in Release 9.2 of Junos OS.

Description

Specify the rules to be used as match criteria.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

match (rulebase-ddos)

Syntax

```
match {
  application [ any | default ];
  application-ddos ddos-application-name;
  destination-address [ address-name ];
  from-zone zone-name;
  source-address [ address-name ];
  to-zone zone-name;
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Specify the rules to be used as match criteria for application-level DDoS protection.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

match (Security Policies)

Syntax

```
match {
  application [ application-name-or-set ];
  destination-address {
    address-name ;
  }
  source-address {
    address-name ;
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure security policy match criteria.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

match (Source NAT)

Syntax

```
match {
   destination-address [destination-address];
   destination-port port-number;
   source-address [source-address];
}
```

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the source rules to be used as match criteria.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

match (Static NAT)

Syntax

```
match {
   destination-address [destination-address];
}
```

Hierarchy Level [edit security nat static rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the static rules to be used as match criteria.

Options The remaining statement is explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-context-values

Syntax

```
context <context-name> {
   max-context-values number;
}
```

Hierarchy Level [edit security idp application-ddos *name* context *context-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description (Optional) Configures the top *n* context values that should be monitored, reported, or both, for application-level DDoS protection.

Options ***number*** —Monitor top *n* context values only.

Range: 1 to 10,000

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-flow-mem

Syntax max-flow-mem *value* ;

Hierarchy Level [edit security idp sensor-configuration re-assembler]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Define the maximum TCP flow memory which IDP sensor can handle.

Options ***value*** —Maximum TCP flow memory in kilobytes.

Range: 64 through 4,294,967,295 kilobytes

Default: 1024 kilobytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

max-logs-operate

Syntax max-logs-operate *value* ;

Hierarchy Level [edit security idp sensor-configuration log suppression]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This setting specifies how many log records are tracked simultaneously by IDP.

Options *value* —Maximum number of log records are tracked by IDP.

Range: 256 through 65536 records

Default: 16384 records

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max–message–length

Syntax max-message-length *number*;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Sets the maximum message payload length (in bytes) the security device accepts for a GTP message. The default maximum message length is 65,535 bytes.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-packet-mem

Syntax max-packet-mem *value* ;

Hierarchy Level [edit security idp sensor-configuration re-assembler]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Define the maximum TCP packet memory that the IDP sensor can handle.

Options *value* —Maximum TCP packet memory.
Range: 64 through 4,294,967,295 kilobytes (KB)
Default: 262144 KB

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-packet-memory

Syntax max-packet-memory *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the maximum memory length of a packet in bytes.

Options *value* —Maximum memory length in bytes.
Range: 0 through 200,000,000 bytes
Default: 100,000,000 bytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

max-session-number

Syntax max-session-number *number*;

Hierarchy Level [edit security nat source rule-set *ruleset* rule *rule* then source-nat (pool | interface) persistent-nat]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description The maximum number of the sessions with which a persistent NAT binding can be associated. For example, if the **max-session-number** of the persistent NAT rule is 100, then a 101th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule.

Options *number*—Maximum number of sessions.

Range: 8 through 100

Default: 30 sessions

Required Privilege Level **security**—To view this statement in the configuration.
security-control—To add this statement to the configuration

Related Documentation
- *Junos OS Security Configuration Guide*

max-sessions

Syntax max-sessions *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]
[edit services application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS. Support for application identification in the services hierarchy added in 10.2.

Description Specify the maximum number of sessions that IDP maintains. If the sensor reaches the maximum, it drops all new sessions.

Options *value* —Maximum number of sessions.

Range: 0 through 500000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-sessions (packet-log)

Syntax max-sessions *percentage*;

Hierarchy Level [edit security idp sensor-configuration packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the maximum number of sessions actively conducting pre-attack packet captures on a device at one time. This value is expressed as a percentage of the maximum number of IDP sessions for the device.

Options *percentage*—Maximum number of packet capture sessions expressed as a percentage of the IDP session capacity for the device.

Range: 1 to 100 percent

Default: 10

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-tcp-session-packet-memory

Syntax max-tcp-session-packet-memory *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the maximum number of TCP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new TCP sessions.

Options *value* —Maximum number of TCP sessions.

Range: 0 through 60000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

max-time-report

Syntax max-time-report *value* ;

Hierarchy Level [edit security idp sensor-configuration log suppression]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description When log suppression is enabled, IDP maintains a count of multiple occurrences of the same event. After the specified number of seconds has passed, IDP writes a single log entry containing the count of occurrences.

Options *value* —Time after which IDP writes a single log entry containing the count of occurrences.

Range: 1 through 60 seconds

Default: 5 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-timers-poll-ticks

Syntax max-timers-poll-ticks *value* ;

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the time at which timer ticks at regular interval.

Options *value* —Maximum amount of time at which the timer ticks.

Range: 0 through 1000 ticks

Default: 1000 ticks

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

max-udp-session-packet-memory

Syntax max-udp-session-packet-memory *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the maximum number of UDP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new UDP sessions.

Options *value* —Maximum number of UDP sessions.

Range: 0 through 20000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

maximize-idp-sessions

Syntax

```
maximize-idp-sessions {
inline-tap;
  weight {
    equal;
    firewall;
    idp;
  }
}
```

Hierarchy Level [edit security forwarding-process application-services]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity. See weight for information about the options provided.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

maximum-call-duration

Syntax maximum-call-duration *minutes* ;

Hierarchy Level [edit security alg mgcp],
[edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the time at which the SIP call ends. The media session is released after the call has ended.

Options *minutes* —Maximum amount of time at which the call ends and releases the media sessions.

Range: 3 through 7200 minutes

Default: 720 minutes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

maximum-message-length

Syntax maximum-message-length *number*;

Hierarchy Level [edit security alg dns]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the maximum DNS message length.

Options **number**—Maximum length in bytes of a single DNS message.

Range: 512 through 8192 bytes.

Default: 512 bytes.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

mcc–mnc (gtp)

Syntax

```
mcc-mnc <mcc-mnc-number> {
  action <drop | pass | selection <ms | net | vrf> {
    }
  }
```

Hierarchy Level

[edit security gprs gtp profile *profile name* apn *pattern-string* mcc-mnc]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

By default, the security device grants access to any International Mobile Station Identity (IMSI) prefix. An IMSI prefix consists of a Mobile Country Code (MCC) and a Mobile Network Code (MNC). The set and unset commands allow or deny specific IMSI prefixes. These commands only apply to create pdp context request GTP messages. The MCC-MNC pair can be five or six digits.

You can filter GTP packets based on the combination of an IMSI prefix and an APN.

- *number*—Specify an IMSI prefix.
- *string*—Specify an APN.
- **drop**—Enable the security device to deny GTP packets from all Selection Modes for the specified APN.
- **selection**—Specify one of the following Selection Modes for the APN:
  - **ms** The APN is provided by a mobile station (MS) and the user-subscription is not verified.
  - **net** The APN is provided by a network and the user-subscription is not verified.
  - **vrf** The APN is provided by a network or an MS and the user-subscription is verified.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

media-source-port-any

Syntax media-source-port-any;

Hierarchy Level [edit security alg h323]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Allow media traffic from any port number. By default, this feature is disabled, which allows a temporary opening in the firewall (pinhole) for media traffic to be opened.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

member (Group VPN)

Syntax

```
member {
  ike {
    gateway gateway-name {
      address [(ip-address | hostname)];
      ike-policy policy-name;
      local-address address;
      local-identity (distinguished-name string | hostname hostname | inet ipv4-ip-address
        | user-at-hostname e-mail-address);
    }
    policy name {
      certificate {
        local-certificate identifier;
        peer-certificate-type [pkcs7 | x509-signature);
        trusted-ca (ca-index | use-all);
      }
      description text;
      mode (aggressive | main);
      pre-shared-key (ascii-text text | hexadecimal hex);
      proposal-set (basic | compatible | standard);
      proposals name;
    }
    proposal name {
      authentication-algorithm (md5 | sha-256 | sha1);
      authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
      description text;
      dh-group (group1 | group2 | group5 | group14);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      lifetime-seconds seconds;
    }
  }
  ipsec vpn name {
    group id;
    group-vpn-external-interface interface;
    heartbeat-threshold number;
    ike-gateway name;
  }
}
```

Hierarchy Level

[edit security group-vpn]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Configure group VPN member.

Options

Configure group VPN member. You configure the following on the group member:

- Phase 1 IKE SA with the group server. The IKE gateway is the group server.

NOTE: We recommend that you do not change the default value for lifetime-seconds for the IKE proposal on the member. Increasing the value

Copyright © 2011, Juniper Networks, Inc.

might cause the member device to continue to use the existing Phase 1 IKE SA key even in the event of a crash; this can delay the recovery process.

- IPsec group VPN.

NOTE: A scope policy must also be configured on the group member. To configure a scope policy, use the **policies** configuration statement at the [**edit security**] hierarchy and specify the IPsec group VPN for the **ipsec-group-vpn** option.

The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

member (IDP)

Syntax

```
member member-name {
  attack-type {
    (anomaly | signature);
  }
}
```

Hierarchy Level
[edit security idp custom-attack *attack-name* attack-type chain]

Release Information
Statement introduced in Release 9.3 of Junos OS.

Description
Create the list of member attacks.

Options
member-name —Name of the member list.

The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

message-flood (H323)

Syntax

```
message-flood {
  gatekeeper threshold rate ;
}
```

Hierarchy Level [edit security alg h323 application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limit the rate per second at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default.

Options

gatekeeper threshold *rate* —Maximum number of RAS connection requests per second allowed per gateway.

Range: 1 through 65,535

Default: 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

message-flood (MGCP)

Syntax

```
message-flood threshold rate ;
```

Hierarchy Level [edit security alg mgcp application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Limits the rate per second at which message requests to the Media Gateway are processed. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG). This feature is disabled by default.

Options

threshold *rate* —Number of connection requests per second allowed per Media Gateway.

Range: 2 through 50000

Default: 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

mgcp

Syntax

```
mgcp {
  application-screen {
    connection-flood threshold rate ;
    message-flood threshold rate ;
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  inactive-media-timeout seconds ;
  maximum-call-duration minutes ;
  traceoptions {
    flag {
      all <extensive>;
      call <extensive>;
      cc <extensive>;
      decode <extensive>;
      error <extensive>;
      nat <extensive>;
      packet <extensive>;
      rm <extensive>;
    }
  }
  transaction-timeout seconds ;
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the Media Gateway Control Protocol (MGCP) ALG on the device. MGCP is a text-based Application Layer protocol that can be used for call setup and call control.

Options **disable**—Disable the MGCP ALG. By default, the MGCP ALG is enabled.

NOTE: By default, the MGCP ALG is disabled for SRX Series devices.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

mime-pattern

Syntax

```
mime-pattern {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass various types of scanning.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

mime-whitelist

Syntax

```
mime-whitelist {
list listname {
   exception listname;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS. Statement updated in 11.1 for Sophos antivirus support.

Description Configure the antivirus scanner to use MIME bypass lists and exception lists.

WARNING: When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

min–message–length

Syntax **min-message-length** *number*;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Sets the minimum message payload length (in bytes) the security device accepts for a GTP message. The default maximum message length is 0 bytes.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

mode (Forwarding-Options)

Syntax mode (packet-based | flow-based | drop);

Hierarchy Level [edit security forwarding-options family inet6]

Release Information Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.

Description Specify forwarding options for IPv6 traffic.

Options **drop**—Drop IPv6 packets. This is the default setting.

flow-based—Perform flow-based packet forwarding.

packet-based—Perform simple packet forwarding. Packet-based mode is not available for SRX3400, SRX3600, SRX5400, or SRX5600. The option does not appear in the CLI for these devices.

If you change the forwarding option mode for IPv6, you might have to perform a reboot to initialize the configuration change. Table 4 on page 579 summarizes device status upon configuration change.

Table 4: Device Status Upon Configuration Change

Configuration Change	Commit Warning	Reboot Required	Impact on Existing Traffic Before Reboot	Impact on New Traffic Before Reboot
Drop to flow-based	Yes	Yes	Dropped	Dropped
Drop to packet-based	No	No	Packet-based	Packet-based
Flow-based to packet-based	Yes	Yes	None	Flow sessions created
Flow-based to drop	Yes	Yes	None	Flow sessions created
Packet-based to flow-based	Yes	Yes	Packet-based	Packet-based
Packet-based to drop	No	No	Dropped	Dropped

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

mode (Policy)

Syntax mode (aggressive | main);

Hierarchy Level [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Define the mode used for Internet Key Exchange (IKE) Phase 1 negotiations. Use aggressive mode only when you need to initiate an IKE key exchange without ID protection, as when a peer unit has a dynamically assigned IP address. (The **main** option is not supported on dynamic VPN implementations.)

Options
- **aggressive**—Aggressive mode.
- **main**—Main mode. Main mode is the recommended key-exchange method because it conceals the identities of the parties during the key exchange.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

mode (Security Logging)

Syntax mode (event | stream)

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server).

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

mpls

Syntax

```
mpls {
   mode packet-based;
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Enable the forwarding of MPLS traffic. By default, the device drops MPLS traffic.

CAUTION: Because MPLS is in operating packet mode, security services are not available.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

msrpc

Syntax

```
msrpc {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the Microsoft (MS) remote procedure call (RPC) ALG on the device.

Options

disable—Disable the Microsoft RPC ALG. By default, the Microsoft RPC ALG is enabled.

traceoptions—Configure the Microsoft RPC ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- **all**—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

mss

Syntax

```
mss {
  match (equal | greater-than | less-than | not-equal);
  value maximum-segment-size;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the maximum segment size (MSS) in the TCP header.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value*maximum-segment-size*—Match the maximum segment size value.

Range: 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

nat

Syntax

```
nat {
  destination {
    pool pool-name {
      address < ip-address > (to ip-address | port port-number );
      routing-instance routing-instance-name ;
    }
    rule-set rule-set-name {
      from interface [interface-name] |
      routing-instance [routing-instance-name] | zone [zone-name];
      rule rule-name {
        match {
          destination-address destination-address ;
          destination-port port-number ;
          source-address [source-address];
        }
        then {
          destination-nat (off | pool pool-name );
        }
      }
    }
  }
  proxy-arp {
    interface interface-name {
      address ip-address to ip-address ;
    }
  }
  source {
    address-persistent;
    interface {
      port-overloading { off };
    }
    pool pool-name {
      address ip-address to ip-address ;
      host-address-base ip-address ;
      overflow-pool (interface | pool-name );
      port no-translation | range high ip-address low ip-address ;
      routing-instance routing-instance-name ;
    }
    pool-utilization-alarm {
      clear-threshold threshold-value ;
      raise-threshold threshold-value ;
    }
    port-randomization {
      disable;
    }
    rule-set rule-set-name {
      from interface [interface-name] |
      routing-instance [routing-instance-name] | zone [zone-name];
      rule rule-name {
        match {
          destination-address [destination-address];
          source-address [source-address];
```


Copyright © 2011, Juniper Networks, Inc.

```
                }
                then {
                  source-nat (off | interface | pool pool-name );
                  persistent-nat {
                    address-mapping;
                    inactivity-timeout seconds;
                    max-session-number number;
                    permit ( any-remote-host | target-host | target-host-port );
                  }
                }
              }
              to interface [interface-name] |
              routing-instance [routing-instance-name] | zone [zone-name];
            }
          }
          static {
            rule-set rule-set-name {
              from interface [interface-name] |
              routing-instance [routing-instance-name] | zone [zone-name];
              rule rule-name {
                match {
                  destination-address [destination-address];
                }
                then {
                  static-nat prefix < addr-prefix >
                  <routing-instance routing-instance-name >;
                }
              }
            }
          }
          traceoptions {
            file filename {
              <files number >;
              <match regular-expression >;
              <size maximum-file-size >;
              <world-readable | no-world-readable>;
            }
            flag {
              all;
              destination-nat-pfe;
              destination-nat-re;
              destination-nat-rt;
              source-nat-pfe;
              source-nat-re;
              source-nat-rt;
              static-nat-pfe;
              static-nat-re;
              static-nat-rt;
            }
            no-remote-trace;
          }
        }
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure Network Address Translation (NAT) for the SRX Series device.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

nat-keepalive

Syntax nat-keepalive *seconds* ;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.

Options *seconds* —Maximum interval in seconds at which NAT keepalive packets can be sent.
Range: 1 through 300 seconds
Default: 5 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

negate

Syntax negate;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Select negate to exclude the specified pattern from being matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

nested-application-identification

Syntax
nested-application-identification
no-nested-application-identification

Hierarchy Level
[edit security idp sensor-configuration application-identification
no-nested-application-identification]

Release Information
Statement introduced in Release 10.1 of Junos OS.

Description
Sometimes there is a need to identify multiple different applications running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols. This function is turned on by default. Use the **no-nested-application-identification** statement to turn it off.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

nested-application-system-cache

Syntax
nested-application-system-cache
no-nested-application-system-cache

Hierarchy Level
[edit security idp sensor-configuration application-identification
no-nested-application-system-cache]

Release Information
Statement introduced in Release 10.1 of Junos OS.

Description
Nested application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-nested-application-system-cache** statement to turn it off.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-allow-icmp-without-flow

See **allow-icmp-without-flow**

no-anti-replay

Syntax no-anti-replay;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike gateway gateway *-name*]
[edit security group-vpn server group *group-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchy added in Release 10.2 of Junos OS.

Description Disable the antireplay checking feature of IPsec. By default, antireplay checking is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-autoupdate

Syntax no-autoupdate;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine pattern-update]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Turn off automatic data file (pattern file) update for the Sophos antivirus engine.

NOTE: The data files used with Sophos are not a typical virus pattern files, they are small file that helps guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

no-enable-all-qmodules

See **enable-all-qmodules**

no-enable-packet-pool

See **enable-packet-pool**

no-log-errors

See **log-errors**

Copyright © 2011, Juniper Networks, Inc.

no-nat-traversal

Syntax no-nat-traversal;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Disables UDP encapsulation of IPsec Encapsulating Security Payload (ESP) packets, otherwise known as Network Address Translation Traversal (NAT-T). NAT-T is enabled by default.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-notify-mail-recipient (fallback-non-block)

Syntax no-notify-mail-recipient;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options fallback-non-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Do not notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback-non-block action occurs.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-notify-mail-sender (fallback-block)

Syntax no-notify-mail-sender;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options fallback-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Do not notify the e-mail sender about errors returned by the antivirus scan engine when a fallback action occurs.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-notify-mail-sender (virus-detection)

Syntax no-notify-mail-sender;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options virus-detection]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Do not notify the e-mail sender when a virus is detected by Sophos antivirus.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-policy-lookup-cache

See **policy-lookup-cache**

no-reset-on-policy

See **reset-on-policy**

Copyright © 2011, Juniper Networks, Inc.

no-sequence-check

Syntax no-sequence-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify that the device does not check sequence numbers in TCP segments during stateful inspection. By default, the device monitors the sequence numbers in TCP segments. The device detects the window scale specified by source and destination hosts in a session and adjusts a window for an acceptable range of sequence numbers according to their specified parameters. The device then monitors the sequence numbers in packets sent between these hosts. If the device detects a sequence number outside this range, it drops the packet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-syn-check

Syntax no-syn-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Disable checking of the TCP SYN bit before creating a session. By default, the device checks that the SYN bit is set in the first packet of a session. If the bit is not set, the device drops the packet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-uri-check

Syntax no-uri-check;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine *profile-name* scan-options]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Do not perform Sophos antivirus Uniform Resource Identifier URI checking. URI checking is performed by analyzing HTTP traffic URI content against a remote Sophos database server to identify malware or malicious content. URI checking is on by default.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-syn-check-in-tunnel

Syntax no-syn-check-in-tunnel;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Disable checking of the TCP SYN bit before creating a session for tunneled packets. By default, the device checks that the SYN bit is set in the first packet of a VPN session. If the bit is not set, the device drops the packet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

notification

Syntax

```
notification {
  log-attacks {
    alert;
  }
  packet-log {
    pre-attack number;
    post-attack number;
    post-attack-timeout seconds;
  }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

Release Information Statement introduced in Release 9.2 of Junos OS. Added packet capture support in Release 10.2 of Junos OS.

Description Configure the logging options against the action. When attacks are detected, you can choose to log an attack and create log records with attack information and send that information to the log server.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

notification-options (antivirus juniper-express-engine)

Syntax

```
notification-options {
virus-detection {
  type (message | protocol-only);
    notify-mail-sender;
    custom-message;
    custom-message-subject;
  }
  fallback-block {
  custom-message;
    custom-message-subject;
    notify-mail-sender;
    type;
  }
  fallback-non-block {
  custom-message;
    custom-message-subject;
    notify-mail-sender;
    type;
  }
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus juniper-express-engine *profile-name*]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

There are multiple notification options you can configure to trigger when a virus is detected.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

notification-options (antivirus kaspersky-lab-engine)

Syntax

```
scan-options {
intelligent-prescreening;
   scan-mode (scan-all | by--extension);
   content-size-limit value;
   timeout value;
   decompress-layer-limit value;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description There are multiple notification options you can configure to trigger when a virus is detected.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

notification-options (antivirus sophos-engine)

Syntax

```
notification-options {
  fallback-block {
    administrator-email email address;
    allow-email;
    custom-message message;
    custom-message-subject subject;
    display-host;
    no-notify-mail-sender;
    notify-mail-sender;
    type (message | protocol-only);
  }
  fallback-non-block {
    custom-message message;
    custom-message-subject subject;
    no-notify-mail-recipient;
    notify-mail-recipient;
  }
  virus-detection {
    custom-message message;
    custom-message-subject subject;
    no-notify-mail-sender;
    notify-mail-sender;
    type (protocol-only | message );
  }
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus sophos-engine *profile-name*]

Release Information

Statement introduced in Release 11.1 of Junos OS.

Description

Configure notifications options for Sophos antivirus. There are multiple notification options you can configure to trigger when a virus is detected.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

notification-options (content-filtering)

Syntax

```
notification-options {
type (message);
   custom-message [message];
}
```

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure a message notification to trigger when a content filter is matched.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

notify-mail-recipient (fallback-non-block)

Syntax notify-mail-recipient;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options fallback-non-block]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback-non-block action occurs.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

notify-mail-sender (antivirus fallback-block)

Syntax notify-mail-sender;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express--engine *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options fallback-block]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description E-mail notification is used to notify the sender or the recipient about the errors returned by either the scan engine or the scan manager when a fallback action occurs.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

notify-mail-sender (antivirus notification-options virus-detection)

Syntax notify-mail-sender;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express--engine *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine *profile-name* notification-options virus-detection]

Release Information Statement introduced in Release 9.5 of Junos OS. Statement updated for Sophos in Release 11.1 of Junos OS.

Description E-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. When a virus is detected, an e-mail is sent to the sender upon virus detection.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

optimized

Syntax optimized;

Hierarchy Level [edit security ipsec vpn *vpn-name* vpn-monitor]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify that the device uses traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default. (This statement is not supported on dynamic VPN implementations.)

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

option

Syntax

```
option {
   match (equal | greater-than | less-than | not-equal);
   value tcp-option;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the TCP option type (kind field in the TCP header).

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value *tcp-option* —Match the option value.

Range: 0 through 255

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

order

Syntax order;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type chain]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound attack object still must match all members, but the attacks or protocol anomalies can appear in random order.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

out-of-resources

Syntax out-of-resources (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted. The default action is BLOCK.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

over-limit

Syntax over-limit (log-and-permit | block);

Hierarchy Level [edit security utm utm-policy *policy-name* traffic-options sessions-per-client]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions and configure an action to occur when the limit is exceeded.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

overflow-pool

Syntax **overflow-pool (*interface* | *pool-name*);**

Hierarchy Level [edit security nat source pool *pool-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify a source pool to use when the current address pool is exhausted. Currently the statement is applicable for IPv4 addresses only.

NOTE: The length of the IPv6 prefix must be 96 when the pool is used for NAT-PT.

Options interface — Interfaces IP address.

pool-name — Defined source pool (created with the **security nat source pool *pool-name*** statement). The source pool must have Port Address Translation (PAT) enabled. PAT is not supported when the address is an IPv6 prefix address.

Required Privilege Level security — To view this statement in the configuration.
security-control — To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

packet-capture

Syntax

```
capture-file file name {
   format pcap
   size size-limit
files number }
```

Hierarchy Level

[edit security datapath-debug]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Sets packet capture for performing the datapath-debug action.

Options

- **format pcap**—Describes the format of the capture file. The default format file is pcap. You can also set it as private (binary) format.
- **size** —Describes the size limit of the capture file.
- **files** —Describes the number of capture files.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

packet-filter

Syntax **packet-filter;**

Hierarchy Level [edit security datapath-debug]

Release Information Command introduced in Release 9.6 of Junos OS; Support for IPv6 addresses for the following options added in Release 10.4 of Junos OS.

- **destination-prefix**
- **source-prefix**

Support for IPv6 filter for the following option added in Release 10.4 of Junos OS

- **interface**

Description Sets packet filter for taking the datapath-debug action. A maximum of four filters are supported at the same time.

Options ***apply-groups***— Groups from which to inherit configuration data.

apply-groups-except— Do not inherit configuration data from these groups.

destination-port— Match TCP/UDP destination port.

destination-prefix— Destination IP address prefix.

interface— Interface name.

protocol— Match IP protocol type.

source-port— Match TCP/UDP source port.

source-prefix— Source IP address prefix.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

packet-log (IDP Policy)

Syntax

```
packet-log {
   pre-attack number;
   post-attack number;
   post-attack-timeout seconds;
}
```

Hierarchy Level [edit security idp idp-policy ***policy-name*** rulebase-ips rule ***rule-name*** then notification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description In response to a rule match, capture the packets received before and after the attack for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack, and limit the duration of post-attack packet capture by specifying a timeout value.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

pair-policy

Syntax pair-policy *pair-policy* ;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Link the policy that you are configuring with another policy that references the same VPN tunnel so that both policies share one proxy ID and one security association (SA). Policy pairing is useful when you want to allow bidirectional traffic over a policy-based VPN that is using source or destination address translation with a dynamic IP address pool or destination address translation with a mapped IP (MIP) or dynamic IP (DIP) address pool.

Without policy pairing, the device derives a different proxy ID from the outbound and inbound policies. Two proxy IDs causes a problem for the remote peer with a single proxy ID for the VPN tunnel.

Pairing two policies solves the proxy ID problem for the remote peer and conserves SA resources. The single proxy ID is derived from the policy you configured last.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

packet-log (Sensor Configuration)

Syntax

```
packet-log {
   total-memory percentage;
   max-sessions percentage;
   source-address ip-address;
   host ip-address port number;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the sensor for packet capture. This configuration defines the amount of memory to be allocated for packet capture and the maximum number of sessions that can generate packet capture data for the device at one time. The configuration also identifies the source address and host address for transmission of the completed packet capture object.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

pass-through

Syntax

```
pass-through {
   access-profile profile-name ;
   client-match match-name ;
   web-redirect;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure pass-through firewall user authentication. The user needs to use an FTP, Telnet, or HTTP client to access the IP address of the protected resource in another zone. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication. Once authenticated, the firewall proxies the connection.

Options

- **access-profile** *profile-name* —(Optional) Name of the access profile.
- **client-match** *match-name* —(Optional) Specify the name of the users or user groups in a profile who are allowed access by this policy. If you do not specify any users or user groups, any user who is successfully authenticated is allowed access.
- **web-redirect**—(Optional) Enable redirecting an HTTP request to the device and redirecting the client system to a webpage for authentication. Including this statement allows users an easier authentication process because they need to know only the name or IP address of the resource they are trying to access.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

password-file

Syntax password-file (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Description Password protected file is the error returned by the scan engine when the scanned file is protected by a password. The default action is log-and-permit.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pattern

Syntax pattern ***signature-pattern*** ;

Hierarchy Level [edit security idp custom-attack ***attack-name*** attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the pattern IDP should match. You construct the attack pattern just as you would when creating a new signature attack object.

Options ***signature-pattern*** —Specify the signature pattern.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pattern-update (kaspersky-lab-engine)

Syntax

```
pattern-update {
  {
    email-notify {
      admin-email
        custom-message
        custom-message-subject
      }
interval value;
  no-autoupdate
  url;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

pattern-update (juniper-express-engine)

Syntax

```
pattern-update {
  {
    email-notify {
      admin-email
        custom-message
        custom-message-subject
      }
interval value;
  no-autoupdate
  url;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

pattern-update (sophos-engine)

Syntax

```
pattern-update {
  email-notify {
    admin–email email address;
    custom-message message;
    custom-message-subject message;
  }
  interval <minutes>;
  no-autoupdate;
  url  <url>;
  }
}
```

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Updates the Sophos pattern data files. You can configure the security device to regularly update the data file automatically, or you can update the file manually.

NOTE: The data files used with Sophos are not a typical virus pattern files, they are small file that helps guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

peer-certificate-type

Syntax peer-certificate-type (pkcs7 | x509-signature);

Hierarchy Level [edit security group-vpn member ike policy *policy-name* certificate]
[edit security group-vpn server ike policy *policy-name* certificate]
[edit security ike policy *policy-name* certificate]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify a preferred type of certificate (PKCS7 or X509). (This statement is not supported on dynamic VPN implementations.)

Options

- **pkcs7**—Public-Key Cryptography Standard #7.
- **x509-signature**—X509 is an ITU-T standard for public key infrastructure.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

perfect-forward-secrecy

Syntax perfect-forward-secrecy keys (group1 | group2 | group5 | group14);

Hierarchy Level [edit security ipsec policy *policy-name*]

Release Information Statement modified in Release 8.5 of Junos OS. Support for group 14 is added in Release 11.1 of Junos OS.

Description Specify Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key. PFS generates each new encryption key independently from the previous key.

Options

group1—Diffie-Hellman Group 1.

group2—Diffie-Hellman Group 2.

group5—Diffie-Hellman Group 5.

group14—Diffie-Hellman Group 14.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

performance

Syntax

```
performance {
   values [fast | normal | slow | unknown];
}
```

Hierarchy Level

[edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify a performance filter to add attack objects based on the performance level that is vulnerable to the attack.

Options

values—Name of the performance filter. You can select from the following performance level:

- **fast**—Fast track performance level.
- **normal**—Normal track performance level.
- **slow**—Slow track performance level.
- **unknown**—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track performance level.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

permit (Persistent NAT)

Syntax permit (any-remote-host | target-host | target-host-port);

Hierarchy Level [edit security nat source rule-set *ruleset* rule *rule* then source-nat (pool | interface) persistent-nat]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Configure persistent NAT mappings.

Options

- **any-remote-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) Any external host can send a packet to the internal host by sending the packet to the reflexive transport address.
- **target-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address.
- **target-host-port**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port.

Required Privilege Level **security**—To view this statement in the configuration.
security-control—To add this statement to the configuration

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

permit (Security Policies)

Syntax

```
permit {
  application-services (redirect-wx | reverse-redirect-wx);
  application-firewall {
    rule-set rule-set-name;
  }
  destination-address {
    drop-translated;
    drop-untranslated;
  }
  firewall-authentication {
    pass-through {
      access-profile profile-name ;
      client-match match-name ;
      web-redirect;
    }
    web-authentication {
      client-match user-or-group ;
    }
  }
  tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name ;
    pair-policy pair-policy ;
  }
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the policy action to perform when packets match the defined criteria.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

permit-command

Syntax permit-command *protocol-command-list*;

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Apply protocol permit command custom-objects to the content-filtering profile

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

persistent-nat

Syntax

```
persistent-nat {
   address-mapping;
   inactivity-timeout seconds;
   max-session-number number;
   permit ( any-remote-host | target-host | target-host-port );
}
```

Hierarchy Level [edit security nat source rule-set *ruleset* rule *rule* then source-nat (pool | interface)]

Release Information Statement introduced in Release 9.6 of Junos OS. Support for address-mapping added in Release 10.2 of Junos OS.

Description Configure persistent NAT.

Options The remaining statements are explained separately.

Required Privilege Level **security**—To view this statement in the configuration.
security-control—To add this statement to the configuration

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

ping-death

Syntax ping-death;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure the device to detect and reject oversized and irregular ICMP packets. Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

pki

Syntax

```
pki {
  auto-re-enrollment {
    certificate-id certificate-id-name {
      ca-profile-name ca-profile-name ;
      challenge-password password ;
      re-enroll-trigger-time-percentage percentage ;
      re-generate-keypair;
    }
  }
  ca-profile ca-profile-name {
    administrator {
      e-mail-address e-mail-address ;
    }
    ca-identity ca-identity ;
    enrollment {
      retry number;
      retry-interval seconds;
      url url-name;
    }
    revocation-check {
      crl {
        disable {
          on-download-failure;
        }
        refresh-interval hours ;
        url url-name ;
      }
      disable;
    }
  }
  traceoptions {
    file filename <files number > <match regular-expression>
    <size maximum-file-size > <world-readable | no-world-readable>
    flag flag ;
  }
}
```

Hierarchy Level

[edit security]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Configure an IPsec profile to request digital certificates.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Feature Guide*
- *Junos OS System Basics and Services Command Reference*

Copyright © 2011, Juniper Networks, Inc.

- *Junos OS Security Configuration Guide*

policies

Syntax

```
policies {
  default-policy {
    (deny-all | permit-all);
  }
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      match {
        application [ application-name-or-set ];
        destination-address {
          address-name ;
        }
        source-address {
          address-name ;
        }
      }
      scheduler-name scheduler-name ;
      then {
        count {
          alarm {
            per-minute-threshold number;
            per-second-threshold number ;
          }
        }
        (deny | reject);
        permit {
          application-services (redirect-wx | reverse-redirect-wx);
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name ;
              client-match match-name ;
              web-redirect;
            }
            web-authentication {
              client-match user-or-group ;
            }
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name ;
            pair-policy pair-policy ;
          }
        }
        log {
          session-close;
          session-init;
        }
      }
    }
```


Copyright © 2011, Juniper Networks, Inc.

```
    }
    policy-rematch;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure network security policies.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

policy (IKE)

Syntax

```
policy policy-name {
  certificate {
    local-certificate certificate-id ;
    peer-certificate-type (pkcs7 | x509-signature);
    trusted-ca ( ca-index | use-all);
  }
  description description ;
  mode (aggressive | main);
  pre-shared-key (ascii-text | hexadecimal);
  proposal-set (basic | compatible | standard);
  proposals [proposal-names];
}
```

Hierarchy Level

[edit security group-vpn member ike]
[edit security group-vpn server ike]
[edit security ike]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description

Configure an IKE policy.

Options

policy-name —Name of the IKE policy. The policy name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

policy (IPsec)

Syntax

```
policy policy-name {
   description description ;
   perfect-forward-secrecy keys (group1 | group2 | group5 | group14);
   proposal-set (basic | compatible | standard);
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement modified in Release 8.5 of Junos OS. Support for group 14 is added in Release 11.1 of Junos OS.

Description Define an IPsec policy.

Options ***policy-name*** —Name of the IPsec policy.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

policy (Security)

Syntax

```
policy policy-name {
  match {
    application [ application-name-or-set ];
    destination-address {
      address-name ;
    }
    source-address {
      address-name ;
    }
  }
  scheduler-name scheduler-name ;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number ;
      }
    }
    (deny | reject);
    permit {
      application-services (redirect-wx | reverse-redirect-wx);
      destination-address {
        drop-translated;
        drop-untranslated;
      }
      destination-nat destination-name ;
      firewall-authentication {
        pass-through {
          access-profile profile-name ;
          client-match match-name ;
          web-redirect;
        }
        web-authentication {
          client-match user-or-group ;
        }
      }
      source-nat (pool pool-name | pool-set pool-set-name | interface);
      tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name ;
        pair-policy pair-policy ;
      }
    }
    log {
      session-close;
      session-init;
    }
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name*]

Copyright © 2011, Juniper Networks, Inc.

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define a security policy.

Options ***policy-name*** —Name of the security policy.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

policy-lookup-cache

Syntax (policy-lookup-cache | no-policy-lookup-cache);

Hierarchy Level [edit security idp sensor-configuration global]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable cache to accelerate IDP policy lookup.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

policy-rematch

Syntax policy-rematch;

Hierarchy Level [edit security policies]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to add a policy that has just been modified to a deferred action list for reevaluation. For every session associated with the policy, the device reevaluates the policy lookup. If the policy is different from the one associated with the session, the device drops the session. If the policy matches, the session continues.

The policy rematch feature is disabled by default.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pool (Destination NAT)

Syntax

```
pool pool-name {
  address < ip-address > (to ip-address | port port-number );
  routing-instance routing-instance-name ;
}
```

Hierarchy Level [edit security nat destination]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Define a destination NAT pool to identify the pool uniquely.

Options *pool-name* —Name of the pool.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pool (Source NAT)

Syntax

```
pool pool-name {
  address ip-address to ip-address ;
  host-address-base ip-address ;
  overflow-pool (interface | pool-name );
  port no-translation | range high ip-address low ip-address ;
  routing-instance routing-instance-name ;
}
```

Hierarchy Level [edit security nat source]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Define a source NAT pool to identify the pool uniquely.

Options *pool-name* —Name of the pool.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

pool-utilization-alarm

Syntax

```
pool-utilization-alarm {
   clear-threshold clear-threshold ;
   raise-threshold raise-threshold ;
}
```

Hierarchy Level [edit security nat source]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Define the pool utilization alarm thresholds for a Network Address Translation (NAT) source IP address pool without Port Address Translation (PAT). When pool utilization exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pop3-profile (antivirus utm-policy)

Syntax pop3-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pop3-profile (content-filtering utm-policy)

Syntax pop3-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering POP3 protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

port

Syntax port no-translation | range high *ip-address* low *ip-address* ;

Hierarchy Level [edit security nat source pool *pool-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the Port Address Translation (PAT) for a source pool.

Options **no-translation**—If set, no Port Address Translation is required.

range high *ip-address* **low** *ip-address* —Specify the port number range attached to each address in the pool.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

port (web filtering)

Syntax port *number*;

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

port-randomization

Syntax
```
port-randomization {
   disable;
}
```

Hierarchy Level [edit security nat source]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Disable random port allocation for pool-based and interface source NAT.

Options **disable**—Disables random port allocation for pool-based and interface source NAT. For pool-based source NAT and interface NAT, port numbers are allocated randomly by default. Although randomized port number allocation can provide protection from security threats such as DNS poison attacks, it can also affect performance and memory usage for pool-based source NAT.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

port-scan

Syntax

```
port-scan {
   threshold number ;
}
```

Hierarchy Level

[edit security screen ids-option *screen-name* tcp]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Prevent port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

Options

threshold *number* —Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. If the number of ports during the threshold period reaches 10 or more, the device rejects additional packets from the source.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

post-attack

Syntax post-attack *number*;

Hierarchy Level [edit security idp idp-policy rulebase-ips rule *rule-name* then notification packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify the number of packets received after an attack that should be captured for further analysis of attacker behavior. If post-attack packets are not significant to your analysis or the configured attack response ends packet transfer, you can set the post-attack option to 0.

Options ***number***—Number of post-attack packets to be captured.

Range: 0 through 255

Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

post-attack-timeout

Syntax post-attack-timeout *seconds*;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify a time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired.

Options ***seconds***—Maximum number of seconds for post-attack packet capture.

Range: 0 to 1800 seconds

Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pptp

Syntax

```
pptp {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the Point-to-Point Tunneling Protocol (PPTP) ALG on the device.

Options

disable—Disable the PPTP ALG. By default, the PPTP ALG is enabled.

traceoptions—Configure PPTP ALG tracing options. To specify more than one trace operation, include multiple flag statements.

flag—Trace operation to perform.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

pre-attack

Syntax pre-attack *number*;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify the number of packets received before an attack that should be captured for further analysis of attacker behavior.

Options ***number***—Number of pre-attack packets.

Range: 1 through 255

Default: 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

pre-filter-shellcode

Syntax pre-filter-shellcode;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Enable to pre-filter the shell code and protects it from buffer overflow attacks. By default this setting is enabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

predefined-attack-groups

Syntax predefined-attack-groups [attack-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks], [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify predefined attack groups that you can use to match the traffic against known attack objects. You can update only the list of attack objects.

Options ***attack-name*** —Name of the predefined attack object group.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

predefined-attacks

Syntax predefined-attacks [attack-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks], [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify predefined attack objects that you can use to match the traffic against known attacks. You can update only the list of attack objects.

Options ***attack-name*** —Name of the predefined attack objects.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

pre-shared-key

Syntax pre-shared-key (ascii-text | hexadecimal);

Hierarchy Level [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy ***policy-name***]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in OS Release 10.2 of Junos OS.

Description Define a preshared key for an IKE policy.

Options **ascii-text**—ASCII text key.

hexadecimal—Hexadecimal key.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

process-ignore-s2c

Syntax process-ignore-s2c;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set the command to disable the server-to-client inspection.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

process-override

Syntax process-override;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set the command to forcefully run the IDS inspection module even if there is no policy match.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

process-port

Syntax process-port *port-number* ;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set the command to a specific port to forcefully run the IDS inspection module on that TCP/UDP port even if there is no policy match.

Options ***port-number*** —Port Number.
Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

products

Syntax

```
products {
   values [list-of-values];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a products filter to add attack objects based on the application that is vulnerable to the attack.

Options **values**—Name of the products filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

profile (antispam sbl)

Syntax

```
profile profile-name{
sbl-default-server;
   spam-action (log-and-permit | block);
   custom-tag-string [***SPAM***];
}
```

Hierarchy Level [edit security utm feature-profile anti-spam sbl]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

profile (antivirus kaspersky-lab-engine)

Syntax

```
profile profile-name {
fallback-options {
  default (log-and-permit | block);
    corrupt-file (log-and-permit | block);
    password-file (log-and-permit | block);
    decompress-layer (log-and-permit | block);
    content-size (log-and-permit | block);
    engine-not-ready (log-and-permit | block);
    timeout (log-and-permit | block);
    out-of-resources (log-and-permit | block);
    too-many-requests (log-and-permit | block);
  }
  scan-options {
  intelligent-prescreening;
    scan-mode (scan-all | by--extension);
    content-size-limit value;
    timeout value;
    decompress-layer-limit value;
  }
  notification-options {
  virus-detection {
    type (message | protocol-only);
      notify-mail-sender;
      custom-message;
    }
    fallback-block {
    custom-message;
      notify-mail-sender;
      type;
    }
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus kaspersky-lab-engine]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Create a profile for the Kaspersky Lab engine. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

profile (antivirus juniper-express-engine)

Syntax

```
profile profile-name {
fallback-options {
  default (log-and-permit | block);
    content-size (log-and-permit | block);
    engine-not-ready (log-and-permit | block);
    timeout (log-and-permit | block);
    out-of-resources (log-and-permit | block);
    too-many-requests (log-and-permit | block);
  }
  scan-options {
  intelligent-prescreening;
    scan-mode (scan-all | by--extension);
    content-size-limit value;
    timeout value;
    decompress-layer-limit value;
  }
  notification-options {
  virus-detection {
    type (message | protocol-only);
      notify-mail-sender;
      custom-message;
    }
    fallback-block {
    custom-message;
      notify-mail-sender;
      type;
    }
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Create a profile for the Juniper express engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

profile (Sophos Antivirus)

Syntax

```
profile <name> {
  fallback-options {
    content-size (block | log-and-permit | permit);
    default (block | log-and-permit | permit);
    engine-not-ready (block | log-and-permit | permit);
    out-of-resource (block | log-and-permit | permit);
    timeout (block | log-and-permit | permit);
    too-many-requests (block | log-and-permit | permit);
  }
  notification-options {
    fallback-block {
      administrator-email email address;
      allow-email;
      custom-message message;
      custom-message-subject subject;
      display-host;
      no-notify-mail-sender;
      notify-mail-sender;
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject subject;
      no-notify-mail-recipient;
      notify-mail-recipient;
    }
    virus-detection {
      custom-message message;
      custom-message-subject subject;
      no-notify-mail-sender;
      notify-mail-sender;
      type (protocol-only | message );
    }
  }
  scan-options {
    content-size-limit value;
    no-uri-check;
    timeout minutes;
    uri-check;
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Create a profile for the Sophos antivirus engine. This profile includes all subsequent configuration options.

 Copyright © 2011, Juniper Networks, Inc.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

profile (content-filtering)

Syntax

```
profile profile-name{
block-command protocol-command-list;
   block-content-type (java-applet | exe | http-cookie);
   block-mime {
   list list-name {
      exception list-name;
      }
   }
permit-command protocol-command-list;
```

Hierarchy Level [edit security utm feature-profile content-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

profile (gtp)

Syntax

```
profile profile name {
  apn pattern-string {
    mcc-mnc <mcc-mnc-number> {
      action <drop | pass | selection <ms | net | vrf> {
        }
      }
  drop {
  aa-create-pdp {
    <0 | 1 | All>;
  }
  aa-delete-pdp {
    <0 | 1 | All>;
  }
  create pdp {
    <0 | 1 | All>;
  }
  data-record {
    <0 | 1 | All>;
  }
  delete-pdp {
    <0 | 1 | All>;
  }
  echo {
    <0 | 1 | All>;
  }
  error-indication {
    <0 | 1 | All>;
  }
  failure-report {
    <0 | 1 | All>;
  }
  fwd-relocation {
    <0 | 1 | All>;
  }
  fwd-srns-context {
    <0 | 1 | All>;
  }
  g-pdu {
    <0 | 1 | All>;
  }
  identification {
    <0 | 1 | All>;
  }
  node-alive {
    <0 | 1 | All>;
  }
  note-ms-present {
    <0 | 1 | All>;
  }
  pdu-notification {
    <0 | 1 | All>;
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
  ran-info {
    <0 | 1 | All>;
  }
  redirection {
    <0 | 1 | All>;
  }
  relocation-cancel {
    <0 | 1 | All>;
  }
  send-route {
    <0 | 1 | All>;
  }
  sgsn-context {
    <0 | 1 | All>;
  }
  supported-extension {
    <0 | 1 | All>;
  }
  update-pdp {
    <0 | 1 | All>;
  }
  ver-not-supported {
    <0 | 1 | All>;
  }
  log {
    forwarded <basic | detail>;
    prohibited <basic | detail>;
    rate-limited <basic | detail>;
      frequency-number <number>;
      }
    state-invalid <basic | detail>;
  }
  max-message-length number;
  min-message-length number;
  rate-limit messages per second;
  remove-r6;
  seq-number-validated;
  timeout <number of hours>;
  }
}
```

Hierarchy Level [edit security gprs gtp]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Create a profile for the gtp feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

profile (SCTP)

Syntax

```
profile name {
  association-timeout time in minutes;
  handshake-timeout time in 10 seconds;
  drop {
    m3ua-service {
      isup;
      sccp;
      tup;
    }
    payload-protocol {
      all;
      asap;
      bicc;
      ddp-segment;
      ddp-stream;
      dua;
      enrp;
      h248;
      h323;
      iua;
      m2pa;
      m2ua;
      m3ua;
      qipc;
      simco;
      sua;
      tali;
      v5ua;
    }
  }
  limit {
    rate {
      address ip-address {
        sccp number;
        ssp number;
        sst number;
      }
      sccp number;
      ssp number;
      sst number;
    }
  }
}
```

Hierarchy Level [edit security gprs]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Create a profile of the Stream Control Transmission Protocol (SCTP) feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

profile (web-filtering surf-control-integrated)

Syntax

```
profile profile-name{
default (log-and-permit | block);
  custom-block-message value;
  fallback-settings {
  default (log-and-permit | block);
    server-connectivity (log-and-permit | block);
    timeout (log-and-permit | block);
    too-many-requests (log-and-permit | block);
  }
  category customurl-list name {
  action (log-and-permit | block);
  }
}
```

Hierarchy Level
[edit security utm feature-profile web-filtering surf-control-integrated]

Release Information
Statement introduced in Release 9.5 of Junos OS.

Description
Create a profile for the web-filtering surf-control-integrated feature. This profile includes all subsequent configuration options.

Options
The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

profile (web-filtering websense-redirect)

Syntax

```
profile profile-name {
server {
host host-name;
   port number;
}
sockets value;
   timeout value;
   fallback-settings {
   default (log-and-permit | block);
      server-connectivity (log-and-permit | block);
      timeout (log-and-permit | block);
      too-many-requests (log-and-permit | block);
   }
}
```

Hierarchy Level

[security utm feature-profile web-filtering websense-redirect]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Create a profile for the web-filtering web-sense feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

profile (web-filtering juniper-local)

Syntax

```
profile profile-name {
default (block | log-and-permit | permit);
  custom-block-message value;
  fallback-settings {
  default (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
}
```

Hierarchy Level

[edit security utm feature-profile web-filtering juniper-local]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Create a profile for the web-filtering juniper–local feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

proposal

Syntax

```
proposal proposal-name {
  authentication-algorithm (md5 | sha1 | sha-256);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description ;
  dh-group (group1 | group2 | group5 | group14);
  encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
  | aes-256-cbc);
  lifetime-seconds seconds;
}
```

Hierarchy Level

[edit security group-vpn member ike]
[edit security group-vpn server ike]
[edit security ike]

Release Information

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for dh-group group 14 and DSA signatures are added in Release 11.1 of Junos OS.

Description

Define an IKE proposal.

Options

proposal-name —Name of the IKE proposal. The proposal name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

proposal-set (IKE)

Syntax proposal-set (basic | compatible | standard);

Hierarchy Level [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify a set of default Internet Key Exchange (IKE) proposals.

Options **basic**—Basic set of two IKE proposals:

- Proposal 1—Preshared key, Data Encryption Standard (DES) encryption, and Diffie-Hellman (DH) group 1 and Secure Hash Algorithm 1 (SHA-1) authentication.
- Proposal 2—Preshared key, DES encryption, and DH group 1 and Message Digest 5 (MD5) authentication.

compatible—Set of four commonly used IKE proposals:

- Proposal 1—Preshared key, triple DES (3DES) encryption, and Gnutella2 (G2) and SHA-1 authentication.
- Proposal 2—Preshared key, 3DES encryption, and DH group 2 and MD5 authentication.
- Proposal 3—Preshared key, DES encryption, and DH group 2 and SHA-1 authentication.
- Proposal 4—Preshared key, DES encryption, and DH group 2 and MD5 authentication.

standard—Standard set of two IKE proposals:

- Proposal 1— Preshared key, 3DES encryption, and DH group 2 and SHA-1 authentication.
- Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and DH group 2 and SHA-1 authentication.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

proposal-set (IPsec)

Syntax proposal-set (basic | compatible | standard);

Hierarchy Level [edit security ipsec policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define a set of default IPsec proposals.

Options **basic**—Basic set of two IPsec proposals:

- Proposal 1—Encapsulating Security Payload (ESP) with no Perfect Forward Secrecy (PFS) security, triple Data Encryption Standard (3DES) encryption, and Secure Hash Algorithm (SHA-1) authentication.
- Proposal 2—ESP with no PFS security, 3DES encryption, and Message Digest 5 (MD5) authentication.

compatible—Set of four commonly used IKE proposals:

- Proposal 1—Preshared key, 3DES encryption, and Gnutella2 (G2) and SHA-1 authentication.
- Proposal 2—Preshared key, 3DES, and Diffie-Hellman (DH) group 2 and MD5 authentication.
- Proposal 3—Preshared key, DES encryption, and DH group 2 and SHA-1 authentication.
- Proposal 4—Preshared key, DES encryption, and DH group 2 and MD5 authentication.

standard—Standard set of two IKE proposals:

- Proposal 1— Preshared key, 3DES encryption, and DH group 2 and SHA-1 authentication.
- Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and DH group 2 and SHA-1 authentication.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

proposals

Syntax proposals [*proposal-names*];

Hierarchy Level [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy ***policy-name***]

Release Information Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify up to four Phase 1 proposals for an IKE policy. If you include multiple proposals, use the same Diffie-Hellman group in all of the proposals.

Options **proposals**—Names of up to four configured Phase 1 proposals.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

protect

Syntax

```
protect {
  deny {
    all | destination-ip address ;
    timeout seconds ;
  }
}
```

Hierarchy Level [edit security alg sip application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure options to protect servers against INVITE attacks.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

protocol (IPsec)

Syntax protocol (ah | esp);

Hierarchy Level [edit security ipsec proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Define the IPsec protocol for a manual or dynamic security association (SA).

Options **ah**—Authentication Header protocol.

esp—Encapsulating Security Payload (ESP) protocol.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

protocol (Manual Security Association)

Syntax protocol (ah | esp)

Hierarchy Level [edit security ipsec vpn *vpn-name* manual]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Define the IPsec protocol for the manual security association. (This statement is not supported on dynamic VPN implementations.)

Options **ah**—Authentication Header protocol.

esp—ESP protocol (To use the ESP protocol, you must also use the **tunnel** statement at the **[edit security ipsec security-association** *sa-name* **mode**] hierarchy level.)

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

protocol (IP Headers in Signature Attack)

Syntax

```
protocol {
   match (equal | greater-than | less-than | not-equal);
   value transport-layer-protocol-id ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the Transport Layer protocol number.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***transport-layer-protocol-id*** —Match the Transport Layer protocol ID.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

protocol (Signature Attack)

Syntax

```
protocol {
  icmp {
    code {
      match (equal | greater-than | less-than | not-equal);
      value code-value ;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length ;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value ;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number ;
    }
    type {
      match (equal | greater-than | less-than | not-equal);
      value type-value ;
    }
  }
  ip {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value hostname ;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value ;
    }
    ip-flags {
      (df | no-df);
      (mf | no-mf);
      (rb | no-rb);
    }
    protocol {
      match (equal | greater-than | less-than | not-equal);
      value transport-layer-protocol-id ;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value hostname ;
    }
    tos {
      match (equal | greater-than | less-than | not-equal);
      value type-of-service-in-decimal ;
    }
    total-length {
      match (equal | greater-than | less-than | not-equal);
      value total-length-of-ip-datagram ;
```

```
    }
    ttl {
      match (equal | greater-than | less-than | not-equal);
      value time-to-live ;
    }
  }
  tcp {
    ack-number {
      match (equal | greater-than | less-than | not-equal);
      value acknowledgement-number ;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value tcp-data-length ;
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port ;
    }
    header-length {
      match (equal | greater-than | less-than | not-equal);
      value header-length ;
    }
    mss {
      match (equal | greater-than | less-than | not-equal);
      value maximum-segment-size ;
    }
    option {
      match (equal | greater-than | less-than | not-equal);
      value tcp-option ;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number ;
    }
    source-port {
      match (equal | greater-than | less-than | not-equal);
      value source-port ;
    }
    tcp-flags {
      (ack | no-ack);
      (fin | no-fin);
      (psh | no-psh);
      (r1 | no-r1);
      (r2 | no-r2);
      (rst | no-rst);
      (syn | no-syn);
      (urg | no-urg);
    }
    urgent-pointer {
      match (equal | greater-than | less-than | not-equal);
      value urgent-pointer ;
    }
    window-scale {
      match (equal | greater-than | less-than | not-equal);
      value window-scale-factor ;
```


Copyright © 2011, Juniper Networks, Inc.

```
        }
        window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size ;
        }
    }
    udp {
        data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length ;
        }
        destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port ;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port ;
        }
    }
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a protocol to match the header information for the signature attack.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

protocol-binding

Syntax

```
protocol-binding {
  application application-name ;
  icmp;
  ip {
    protocol-number transport-layer-protocol-number ;
  }
  rpc {
    program-number rpc-program-number ;
  }
  tcp {
    minimum-port port-number maximum-port port-number ;
  }
  udp {
    minimum-port port-number maximum-port port-number ;
  }
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type chain]
[edit security idp custom-attack *attack-name* attack-type signature]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Select a protocol that the attack uses to enter your network.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

protocol-command

Syntax

```
protocol-command {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

protocol-name

Syntax

```
protocol-name protocol-name {
  tunable-name tunable-name {
    tunable-value protocol-value ;
  }
}
```

Hierarchy Level [edit security idp sensor-configuration detector]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the name of the protocol to be used to configure each of the protocol detector engines.

Options ***protocol-name*** —Name of the specific protocol.

The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

protocols (Interface Host-Inbound Traffic)

Syntax

```
protocols {
  protocol-name ;
  protocol-name <except>;
}
```

Hierarchy Level

[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the types of routing protocol traffic that can reach the device on a per-interface basis.

Options

protocol-name —Protocol for which traffic is allowed. The following protocols are supported:

- **all**—Enable traffic from all possible protocols available.
- **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) Protocol traffic.
- **bgp**—Enable incoming BGP traffic.
- **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
- **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
- **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
- **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
- **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
- **ospf**—Enable incoming OSPF traffic.
- **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
- **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
- **rip**—Enable incoming RIP traffic.
- **router-discovery**—Enable incoming router discovery traffic.
- **rsvp**—Enable incoming Resource Resolution Protocol (RSVP) traffic (IP protocol number 46).
- **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**.
- **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

except—(Optional) except can only be used if all has been defined.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

protocols (Zone Host-Inbound Traffic)

Syntax

```
protocols {
  protocol-name ;
  protocol-name <except>;
}
```

Hierarchy Level [edit security zones security-zone *zone-name* host-inbound-traffic]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the types of traffic that can reach the device for all interfaces in a zone.

Options *protocol-name* —Protocol for which traffic is allowed. The following protocols are supported:

- **all**—Enable traffic from all possible protocols available.
- **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) protocol traffic.
- **bgp**—Enable incoming BGP traffic.
- **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
- **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
- **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
- **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
- **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
- **ospf**—Enable incoming OSPF traffic.
- **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
- **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
- **rip**—Enable incoming RIP traffic.
- **router-discovery**—Enable incoming router discovery traffic.
- **rsvp**—Enable incoming Resource Reservation Protocol (RSVP) traffic (IP protocol number 46).
- **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**. New addresses and ports can be added dynamically. This information must be propagated to the Packet Forwarding Engine (PFE).
- **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

except—(Optional) except can only be used if all has been defined.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

Related Documentation
- *Junos OS Security Configuration Guide*

proxy-arp

Syntax

```
proxy-arp {
  interface interface-name {
    address ip-address to ip-address ;
  }
}
```

Hierarchy Level [edit security nat]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure Address Resolution Protocol (ARP) proxy.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

proxy-identity

Syntax

```
proxy-identity {
  local ip-prefix ;
  remote ip-prefix ;
  service service-name ;
}
```

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Optionally specify the IPsec proxy ID to use in negotiations. The default behavior is to use the identities taken from the firewall policies.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

raise-threshold

Syntax raise-threshold *raise-threshold* ;

Hierarchy Level [edit security nat source pool-utilization-alarm]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the upper threshold at which an SNMP trap is triggered when pool utilization for a source pool without Port Address Translation (PAT) rises above the threshold.This feature is disabled by default.

Options *raise-threshold* —Threshold at which an SNMP trap is triggered.

Range: 50 through 100

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rate-limit

Syntax rate-limit *messages per second*;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description The **rate-limit** command is used to limit the rate of control traffic to any GSN defined in a GTP profile. The **rate-limit** setting range is 1 through 80,000 messages per second.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

real

Syntax

```
real {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the RealAudio and RealVideo ALG on the device.

Options

disable—Disable the RealAudio and RealVideo ALG.

traceoptions—Configure RealAudio and RealVideo ALG tracing options. By default, the RealAudio and RealVideo ALG is enabled.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all RealAudio and RealVideo ALG events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

re-assembler

Syntax

```
re-assembler {
  ignore-mem-overflow;
  max-flow-mem value ;
  max-packet-mem value ;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure TCP reassembler for IDP sensor settings.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

re-enroll-trigger-time-percentage

Syntax re-enroll-trigger-time-percentage ***percentage*** ;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id ***certificate-id-name***]

Release Information Statement modified in Release 9.0 of Junos OS.

Description Specify the time before expiration as a percentage.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

recommended

Syntax **recommended;**

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify recommended filter to add predefined attacks recommended by Juniper to the dynamic attack group.

Options **values**—Name of the recommended filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

recommended-action

Syntax **recommended-action (close | close-client | close-server | drop | drop-packet | ignore | none);**

Hierarchy Level [edit security idp custom-attack *attack-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description When the security device detects an attack, it performs the specified action.

Options The seven actions are as follows, from most to least severe:

close—Reset the client and the server.

close-client—Reset the client.

close-server—Reset the server.

drop—Drop the particular packet and all subsequent packets of the flow.

drop-packet—Drop the particular packet of the flow.

ignore—Do not inspect any further packets.

none—Do not perform any action.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

regexp

Syntax regexp *regular-expression* ;

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a Perl Compatible Regular Expression (PCRE) expression.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

reject

Syntax reject;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Block the service at the firewall. The device drops the packet and sends a TCP reset (RST) segment to the source host for TCP traffic and an ICMP "destination unreachable, port unreachable" message (type 3, code 3) for UDP traffic. For types of traffic other than TCP and UDP, the device drops the packet without notifying the source host, which is also what occurs when the action is **deny**.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

reject-timeout

Syntax reject-timeout *value* ;

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the amount of time in milliseconds within which a response must be received.

Options *value* —Maximum amount of time in milliseconds.
Range: 1 through 65,535 milliseconds
Default: 300 milliseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

remote

Syntax remote *ip-prefix*;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike proxy-identity]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description Specify the remote IPv4 or IPv6 address and subnet mask for the proxy identity.

Options *ip-prefix* —IPv4 or IPv6 address and subnet mask.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

remote-exceptions

Syntax

```
remote-exceptions {
   ip-address/mask;
}
```

Hierarchy Level [edit security dynamic-vpn clients *configuration-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to specify exceptions to the remote protected resources list for the specified dynamic VPN configuration. Traffic to the specified IP address will not go through the dynamic VPN tunnel and therefore will not be protected by the firewall's security policies.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

remote-protected-resources

Syntax

```
remote-protected-resources {
   ip-address/mask;
}
```

Hierarchy Level [edit security dynamic-vpn clients *configuration-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to specify which resources to protect using the dynamic VPN feature. Traffic to the protected resource will go through the specified dynamic VPN tunnel and will therefore be protected by the firewall's security policies.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

remove-r6

Syntax remove-r6;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable the security device to detect and remove 3G-specific attributes from the GTP packet header when the packet passes into a 2G network. This allows you to retain interoperability when roaming between 2G and 3G networks.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

reset

Syntax reset;

Hierarchy Level [edit security idp custom-attack ***attack-name*** attack-type chain]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Select **reset** if the compound attack should be matched more than once within a single session or transaction.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

reset-on-policy

Syntax (reset-on-policy | no-reset-on-policy);

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description IDP keeps track of connections in a table. If enabled, the security module resets the flow table each time a security policy loads or unloads. If this setting is disabled, then the security module continues to retain a previous security policy until all flows referencing that security policy go away. Juniper Networks recommends that you keep this setting enabled to preserve memory.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

respond-bad-spi

Syntax respond-bad-spi *number* ;

Hierarchy Level [edit security ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable response to invalid IPsec Security Parameter Index (SPI) values. If the security associations (SAs) between two peers of an IPsec VPN become unsynchronized, the device resets the state of a peer so that the two peers are synchronized.

Options *number* —Number of times to respond to invalid SPI values per gateway.

Range: 1 through 30

Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

retain-hold-resource

Syntax retain-hold-resource;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to not free media resources for a Session Initiation Protocol (SIP) Application Layer Gateway (ALG), even when a media stream is placed on hold. By default, media stream resources are released when the media stream is held.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

revocation-check

Syntax

```
revocation-check {
  crl {
    disable {
      on-download-failure;
    }
    refresh-interval hours ;
    url url-name ;
  }
  disable;
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Specify the method the device uses to verify the revocation status of digital certificates.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

route-change-timeout

Syntax route-change-timeout *seconds* ;

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the session timeout value on a route change to a nonexistent route. By default, this feature is disabled. If the timeout is not defined, sessions discovered to have no route are aged out by means of their current session timeout values.

Options ***seconds*** —Amount of time before sessions with no route are aged out.

Range: 6 through 1800 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

routing-instance (Destination NAT)

Syntax routing-instance *routing-instance-name* ;

Hierarchy Level [edit security nat destination pool *pool-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the routing instance on which to perform the route lookup for the address in the pool. It is not a mandatory flag. If the user does not configure the routing instance, by default the pool belongs to routing-instance **inet.0**.

Options ***routing-instance-name*** —Name of the routing instance.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

routing-instance (Source NAT)

Syntax routing-instance *routing-instance-name* ;

Hierarchy Level [edit security nat source pool *pool-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the routing instance to which the pool is bound. It is not a mandatory flag. If the user does not configure the routing instance, by default the pool belongs to routing-instance **inet.0**.

Options *routing-instance-name* —Name of the routing instance.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rpc

Syntax
```
rpc {
   program-number rpc-program-number ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the attack for a specified remote procedure call (RPC) program number.

Options **program-number** *rpc-program-number* —RPC program number.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rsh

Syntax

```
rsh {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the remote shell (RSH) ALG on the device.

Options

disable—Disable the RSH ALG. By default, the RSH ALG is enabled.

traceoptions—Configure RSH ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rst-invalidate-session

Syntax rst-invalidate-session;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to mark a session for immediate termination when it receives a TCP reset (RST) message. By default, this feature is disabled and the device applies the normal session timeout interval. For TCP, normal session timeout is 30 minutes; for HTTP, it is 5 minutes; and for UDP, it is 1 minute.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rst-sequence-check

Syntax rst-sequence-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Verify that the TCP sequence number in a TCP segment with the RST bit enabled matches the previous sequence number for a packet in that session or is the next higher number incrementally. If the sequence number does not match either of these expected numbers, the device drops the packet and sends the host a TCP ACK message with the correct sequence number. By default, this check is disabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rtsp

Syntax

```
rtsp {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the Real-Time Streaming Protocol (RTSP) ALG on the device.

Options

disable—Disable the RTSP ALG. By default, the RTSP ALG is enabled.

traceoptions—Configure RTSP ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule (Application Firewall)

Syntax

```
rule rule-name {
  match {
    dynamic-application [dynamic-application-names];
  }
  then {
    permit | deny;
  }
}
```

Hierarchy Level [edit security application-firewall rule-set *rule-set-name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Define a rule within the application firewall rule set.

Options *rule-name* —Name of the application firewall rule.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

rule (Application-Level DDoS Rulebase)

Syntax

```
rule rule-name {
   description text ;
   match {
      application [ any | default ];
      application-ddos ddos-application-name;
      destination-address [ address-name ];
      from-zone zone-name;
      source-address [ address-name ];
      to-zone zone-name;
   }
   then {
      action <close-server | drop-connection | drop-packet | no-action>;
      ip-action {
         <ip-block | ip-close | ip-notify>
         timeout secconds;
      }
   }
}
```

Hierarchy Level

[edit security idp idp-policy ***policy-name*** rulebase-ddos]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure application-level DDoS rule match criteria, and the action to be taken on attack clients.

Options

rule-name—Name of the DDoS rulebase rule.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule (Destination NAT)

Syntax

```
rule rule-name {
  match {
    destination-address destination-address ;
    destination-port port-number ;
    source-address [source-address];
  }
  then {
    destination-nat (off | pool pool-name );
  }
}
```

Hierarchy Level [edit security nat destination rule-set *rule-set-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Define a destination NAT rule.

Options *rule-name* —Name of the destination NAT rule.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

rule (Exempt Rulebase)

Syntax

```
rule rule-name {
  description text ;
  match {
    attacks {
      custom-attacks [ attack-name ];
      predefined-attack-groups [ attack-name ];
      predefined-attacks [ attack-name ];
    }
    destination-address [ address-name ];
    destination-except [ address-name ];
    from-zone zone-name ;
    source-address [ address-name ];
    source-except [ address-name ];
    to-zone zone-name ;
  }
}
```

Hierarchy Level

[edit security idp idp-policy *policy-name* rulebase-exempt]

Release Information

Statement introduced in Release 9.2 of Junos OS.

Description

Specify exempt rule to create, modify, delete, and reorder the rules in a rulebase.

Options

rule-name —Name of the exempt rulebase rule.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule (IPS Rulebase)

Syntax

```
rule rule-name {
  description text ;
  match {
    attacks {
      custom-attacks [ attack-name ];
      predefined-attack-groups [ attack-name ];
      predefined-attacks [ attack-name ];
    }
    destination-address [ address-name ];
    destination-except [ address-name ];
    from-zone zone-name ;
    source-address [ address-name ];
    source-except [ address-name ];
    to-zone zone-name ;
  }
  terminal;
  then {
    action {
      (close-client | close-client-and-server | close-server |
      drop-connection | drop-packet | ignore-connection |
      mark-diffserv value | no-action | recommended);
    }
    ip-action {
      (ip-block | ip-close | ip-notify);
      log;
      target (destination-address | service | source-address |
      source-zone | zone-service);
      timeout seconds ;
    }
    notification {
      log-attacks {
        alert;(
      }
      packet-log {
        pre-attack number;
        post-attack number;
        post-attack-timeout seconds;
      }
    }
    severity (critical | info | major | minor | warning);
  }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify IPS rule to create, modify, delete, and reorder the rules in a rulebase.

Options *rule -name* —Name of the IPS rulebase rule.

The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

rule (Source NAT)

Syntax

```
rule rule-name {
  match {
    destination-address [destination-address];
    source-address [source-address];
  }
  then {
    source-nat (off | interface | pool pool-name );
    persistent-nat {
      address-mapping;
      inactivity-timeout seconds;
      max-session-number number;
      permit ( any-remote-host | target-host | target-host-port );
    }
  }
}
```

Hierarchy Level
[edit security nat source rule-set *rule-set-name*]

Release Information
Statement modified in Release 9.6 of Junos OS.

Description
Define a source NAT rule.

Options
rule-name —Name of the source NAT rule.

The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule (Static NAT)

Syntax

```
rule rule-name {
  match {
    destination-address [destination-address];
  }
  then {
    static-nat prefix < addr-prefix >
    <routing-instance routing-instance-name >;
  }
}
```

Hierarchy Level [edit security nat static rule-set *rule-set-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Define a static NAT rule.

Options *rule-name* —Name of the static NAT rule.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

rulebase-ddos

Syntax

```
rulebase-ddos {
  rule rule-name {
    description text ;
    match {
      application [ any | default ];
      application-ddos ddos-application-name;
      destination-address [ address-name ];
      from-zone zone-name;
      source-address [ address-name ];
      to-zone zone-name;
    }
    then {
      action <close-server | drop-connection | drop-packet | no-action>;
      ip-action {
        <ip-block | ip-close | ip-notify>;
        timeout secconds;
      }
    }
  }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the rulebase parameters for application-level DDoS attacks.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule-set (Application Firewall)

Syntax

```
rule-set {
  rule-set-name {
    rule rule-name  {
      match {
        dynamic-application [dynamic-application-names];
      }
      then {
        permit | deny;
      }
    }
    default-rule {
      permit | deny;
    }
  }
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the set of rules for the application firewall.

Options *rule-set-name*—Name of the rule set.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

rule-set (Destination NAT)

Syntax

```
rule-set rule-set-name {
  from interface [interface-name] |
  routing-instance [routing-instance-name] | zone [zone-name];
  rule rule-name {
    match {
      destination-address destination-address ;
      destination-port port-number ;
      source-address [source-address];
    }
    then {
      destination-nat (off | pool pool-name );
    }
  }
}
```

Hierarchy Level [edit security nat destination]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure the set of rules for destination NAT.

Options *rule-set-name* —Name of the rule set.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rule-set (Source NAT)

Syntax

```
rule-set rule-set-name {
  from interface [interface-name] |
  routing-instance [routing-instance-name] | zone [zone-name];
  rule rule-name {
    match {
      destination-address [destination-address];
      source-address [source-address];
    }
    then {
      source-nat (off | interface | pool pool-name );
      persistent-nat {
        address-mapping;
        inactivity-timeout seconds;
        max-session-number number;
        permit ( any-remote-host | target-host | target-host-port );
      }
    }
  }
  to interface [interface-name] |
  routing-instance [routing-instance-name] | zone [zone-name];
}
```

Hierarchy Level [edit security nat source]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure the set of rules for source NAT.

Options ***rule-set-name*** —Name of the rule set.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

rule-set (Static NAT)

Syntax

```
rule-set rule-set-name {
  from interface [interface-name] |
  routing-instance [routing-instance-name] | zone [zone-name];
  rule rule-name {
    match {
      destination-address [destination-address];
    }
    then {
      static-nat prefix < addr-prefix >
      <routing-instance routing-instance-name >;
    }
  }
}
```

Hierarchy Level

[edit security nat static]

Release Information

Statement modified in Release 9.6 of Junos OS.

Description

Configure the set of rules for static NAT.

Options

rule-set-name —Name of the rule set.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

rulebase-exempt

Syntax

```
rulebase-exempt {
  rule rule-name {
    description text ;
    match {
      attacks {
        custom-attacks [ attack-name ];
        predefined-attack-groups [ attack-name ];
        predefined-attacks [ attack-name ];
      }
      destination-address [ address-name ];
      destination-except [ address-name ];
      from-zone zone-name ;
      source-address [ address-name ];
      source-except [ address-name ];
      to-zone zone-name ;
    }
  }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure the exempt rulebase to skip detection of a set of attacks in certain traffic.

NOTE: You must configure the IPS rulebase before configuring the exempt rulebase.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

rulebase-ips

Syntax

```
rulebase-ips {
  rule rule-name {
    description text ;
    match {
      attacks {
        custom-attacks [ attack-name ];
        predefined-attack-groups [ attack-name ];
        predefined-attacks [ attack-name ];
      }
      destination-address [ address-name ];
      destination-except [ address-name ];
      from-zone zone-name ;
      source-address [ address-name ];
      source-except [ address-name ];
      to-zone zone-name ;
    }
    terminal;
    then {
      action {
        (close-client | close-client-and-server | close-server |
        drop-connection | drop-packet | ignore-connection |
        mark-diffserv value | no-action | recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        target (destination-address | service | source-address |
        source-zone | zone-service);
        timeout seconds;
      }
      notification {
        log-attacks {
          alert;(
        }
        packet-log {
          pre-attack number;
          post-attack number;
          post-attack-timeout seconds;
        }
      }
      severity (critical | info | major | minor | warning);
    }
  }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure the IPS rulebase to detect attacks based on stateful signature and protocol anomalies.

Copyright © 2011, Juniper Networks, Inc.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sbl

Syntax

```
sbl {
profile profile-name{
  sbl-default-server;
    spam-action (log-and-permit | block);
    custom-tag-string [***SPAM***];
  }
  address-whitelist{
  listname;
  }
}
```

Hierarchy Level [edit security utm feature-profile anti-spam]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure UTM server-based antispam features.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sbl-default-server

Syntax sbl-default-server;

Hierarchy Level [edit security utm feature-profile anti-spam sbl profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the default SBL server lookup as enabled or disabled. If you are using server-based spam filtering, you should enter *sbl-default-server* to enable the default SBL server. (The SBL server is predefined on the device. It ships with the name and address of the SBL server.)

Options
- sbl-default-server—Enable server-based spam filtering
- no-sbl-default-server—Disable server-based spam filtering. You would disable it if you are using only local lists or if you do not have a license for server-based spam filtering.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

scan-mode

Syntax scan-mode (scan-all | by-extension);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* scan-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can scan all content or scan content with specific file extensions. You can use a file extension list to define a set of file extensions that are used in file extension scan mode. The antivirus module can then only scan files with extensions on the scan-extension list.

Options
- scan-all—Scan all files.
- by–extension—Scan only files with extensions specified in a file extension list custom object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

scan-options (antivirus juniper-express-engine)

Syntax

```
scan-options {
intelligent-prescreening;
   scan-mode (scan-all | by--extension);
   content-size-limit value;
   timeout value;
   decompress-layer-limit value;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the anti-virus feature to scan specific types of traffic based on various scanning configuration parameters.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

scan-options (anti-virus kaspersky-lab-engine)

Syntax

```
scan-options {
intelligent-prescreening;
   scan-mode (scan-all | by--extension);
   content-size-limit value;
   timeout value;
   decompress-layer-limit value;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

sccp

Syntax

```
sccp {
  application-screen {
    call-flood threshold rate ;
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  inactive-media-timeout seconds ;
  traceoptions {
    flag {
      all <extensive>;
      call <extensive>;
      cc <extensive>;
      cli <extensive>;
      decode <extensive>;
      error <extensive>;
      init <extensive>;
      nat <extensive>;
      rm <extensive>;
    }
  }
}
```

Hierarchy Level

[edit security alg]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the Skinny Client Control Protocol (SCCP) ALG on the device.

Options

disable—Disable the SCCP ALG. By default, the SCCP ALG is enabled.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

scheduler-name

Syntax scheduler-name *scheduler-name* ;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the schedule (as defined by the **scheduler** *scheduler-name* statement) for which the policy is in effect.

Options *scheduler-name* —Name of the scheduler.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

scope (Chain Attack)

Syntax scope (session | transaction);

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type chain]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify whether the match should occur over a single session or can be made across multiple transactions within a session.

Options **session**—Allow multiple matches for the object within the same session.

transaction—Match the object across multiple transactions that occur within the same session.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

scope (Custom Attack)

Syntax scope (destination | peer | source);

Hierarchy Level [edit security idp custom-attack *attack-name* time-binding]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify whether the counting of the attack is from the same source IP address, the same destination IP address, or a peer.

Options

- **destination**—IDP detects attacks to a given destination IP address for the specified number of times, regardless of the source IP address.
- **peer**—IDP detects attacks between source and destination IP addresses of the sessions for the specified number of times.
- **source**—IDP detects attacks from a given source IP address for the specified number of times, regardless of the destination IP address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

screen (Security)

Syntax

```
screen {
  ids-option screen-name {
    alarm-without-drop;
      icmp {
        flood {
          threshold number ;
        }
        fragment;
        ip-sweep {
          threshold number ;
        }
        large;
        ping-death;
      }
      ip {
        bad-option;
        block-frag;
        loose-source-route-option;
        record-route-option;
        security-option;
        source-route-option;
        spoofing;
        stream-option;
        strict-source-route-option;
        tear-drop;
        timestamp-option;
        unknown-protocol;
      }
      limit-session {
        destination-ip-based number ;
        source-ip-based number ;
      }
      tcp {
        fin-no-ack;
        land;
        port-scan {
          threshold number ;
        }
        syn-ack-ack-proxy {
          threshold number ;
        }
        syn-fin;
        syn-flood {
          alarm-threshold number ;
          attack-threshold number ;
          destination-threshold number ;
          source-threshold number ;
          timeout seconds ;
        }
        syn-frag;
        tcp-no-flag;
        tcp-sweep {
```

```
                threshold threshold number;
              }
              winnuke;
            }
            udp {
              flood {
                threshold number ;
              }
              udp-sweep {
                threshold threshold number;
              }
            }
          }
          traceoptions {
            file filename <files number > <match regular-expression >
            <size maximum-file-size > <world-readable | no-world-readable>;
            flag flag ;
          }
        }
      }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure security screen options.

Options *screen-name* —Name of the screen configured at **security screen ids-options** level.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

screen (Zones)

Syntax screen *screen-name* ;

Hierarchy Level [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify a security screen for a security zone.

Options *screen-name* —Name of the screen.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

sctp

Syntax

```
sctp {
  log {
    configuration;
    decoding-error;
    dropped-packet;
    exceeding-rate-limit;
  }
  profile name {
    association-timeout time in minutes;
    handshake-timeout time in seconds;
    drop {
      m3ua-service {
        isup;
        sccp;
        tup;
      }
      payload-protocol {
        all;
        asap;
        bicc;
        ddp-segment;
        ddp-stream;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
        simco;
        sua;
        tali;
        v5ua;
      }
    }
    limit {
      rate {
        address ip-address {
          sccp number;
          ssp number;
          sst number;
        }
        sccp number;
        ssp number;
        sst number;
      }
    }
  }
  traceoptions {
    file;
```


Copyright © 2011, Juniper Networks, Inc.

```
        flag {
          all;
          chassis-cluster;
          configuration;
          flow;
          parser;
        }
      }
    }
```

Hierarchy Level [edit security gprs]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Use the Stream Control Transmission Protocol (SCTP) commands to configure SCTP objects, configure SCTP logs, set trace options, and set address rate limit.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

security-package

Syntax

```
security-package {
  automatic {
    download-timeout;
    enable;
    interval hours ;
    start-time start-time ;
  }
  url url-name ;
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure the device to automatically download the updated signature database from the specified URL.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

security-zone

Syntax

```
security-zone zone-name {
  address-book {
    address address-name (ip-prefix | dns-name dns-address-name | wildcard-address
      ipv4–address/wildcard-mask);
    address-set address-set-name {
      address address-name ;
    }
  }
  host-inbound-traffic {
    protocols {
      protocol-name ;
      protocol-name <except>;
    }
    system-services {
      service-name ;
      service-name < except >;
    }
  }
  interfaces interface-name {
    host-inbound-traffic {
      protocols {
        protocol-name ;
        protocol-name < except >;
      }
      system-services {
        service-name ;
        service-name < except >;
      }
    }
  }
  screen screen-name ;
  tcp-rst;
}
```

Hierarchy Level

[edit security zones]

Release Information

Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description

Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.

Options

zone-name —Name of the security zone.

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

sensor-configuration

Syntax

```
sensor-configuration {
  application-identification {
    application-system-cache;
    application-system-cache-timeout value ;
    disable;
    max-packet-memory value ;
    max-sessions value ;
    max-tcp-session-packet-memory value ;
    max-udp-session-packet-memory value ;
    nested-application-system-cache;
    nested-application;
  }
  detector {
    protocol-name protocol-name {
      tunable-name tunable-name {
        tunable-value protocol-value ;
      }
    }
  }
  flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    (log-errors | no-log-errors);
    max-timers-poll-ticks value ;
    reject-timeout value ;
    (reset-on-policy | no-reset-on-policy);
  }
  global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    (policy-lookup-cache | no-policy-lookup-cache);
  }
  ips {
    detect-shellcode;
    ignore-regular-expression;
    log-supercede-min minimum-value ;
    pre-filter-shellcode;
    process-ignore-s2c;
    process-override;
    process-port port-number ;
  }
  log {
    cache-size size ;
    suppression {
      disable;
      include-destination-address;
      max-logs-operate value ;
      max-time-report value ;
      start-log value ;
    }
  }
  packet-log {
    total-memory percentage;
```

```
        max-sessions percentage;
        source-address ip-address;
        host ip-address port number ;
    }
    re-assembler {
        ignore-mem-overflow;
        max-flow-mem  value ;
        max-packet-mem  value ;
    }
    ssl-inspection {
        sessions  number ;
    }
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure various IDP parameters to match the properties of transiting network traffic.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

seq-number-validated

Syntax **seq-number-validated;**

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable or disable the GTP Sequence Number Validation feature.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

server

Syntax

```
server {
host host-name;
   port number;
}
```

Hierarchy Level

[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Set server parameters by entering the server name or IP address.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

server-connectivity

Syntax

server-connectivity (log-and-permit | block);

Hierarchy Level

[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Fallback settings tell the system how to handle errors. This is the action that occurs when a request fails for this reason.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

sessions

Syntax sessions *number* ;

Hierarchy Level [edit security idp sensor-configuration ssl-inspection]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Maximum number of SSL sessions for inspection. This limit is per Services Processing Unit (SPU).

Options *number* —Number of SSL session to inspect.

Range: 1 through 100000

Default: 10000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

session-close

Syntax session-close;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then log]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable traffic to which the policy applies to be logged at the end of a session.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

session-init

Syntax session-init;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then log]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable traffic to which the policy applies to be logged at the beginning of a session.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sessions-per-client

Syntax

```
sessions-per-client {
limit value;
   over-limit (log-and-permit | block);
}
```

Hierarchy Level [edit security utm utm-policy *policy-name* traffic-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sequence-number (ICMP Headers in Signature Attack)

Syntax

```
sequence-number {
   match (equal | greater-than | less-than | not-equal);
   value sequence-number;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***sequence-number*** —Match a decimal value.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

sequence-number (TCP Headers in Signature Attack)

Syntax

```
sequence-number {
   match (equal | greater-than | less-than | not-equal);
   value sequence-number;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***sequence-number*** —Match a decimal value.

Range: 0 through 4,294,967,295

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

server (Group VPN)

Syntax

```
server {
  group name{
    activation-time-delay seconds;
    anti-replay-time-window seconds;
    description text;
    group-id number;
    ike-gateway gateway-name;
    ipsec-sa name {
      proposal name;
        match-policy name {
          destination ip-address/netmask;
          destination-port number;
          protocol number;
          source ip-address/netmask;
          source-port number;
      }
    }
    no-anti-replay;
    server-address ip-address;
    server-member-communication {
      certificate certificate-id;
      communication-type (multicast | unicast);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      heartbeat seconds;
      lifetime-seconds seconds;
      multicast-group address;
      multicast-outgoing-interface interface;
      number-of-retransmission number;
      retransmission-period seconds;
      sig-hash-algorithm (md5 | sha1);
    }
  }
  ike {
    gateway name {
      address ( ip-address | hostname );
      dynamic {
        distinguished-name {
          container string;
          wildcard string;
        }
        hostname name;
        inet ip-address;
        user-at-hostname email-address;
      }
      ike-policy name;
      local-identity {
        distinguished-name;
        hostname name;
        inet ip-address;
        user-at-hostname emailaddress;
      }
    }
```

```
    policy name {
      certificate {
        local-certificate identifier;
        peer-certificate-type [pkcs7 | x509-signature);
        trusted-ca (ca-index | use-all);
      }
      description text;
      mode (aggressive | main);
      pre-shared-key (ascii-text text | hexadecimal hex);
      proposal-set (basic | compatible | standard);
      proposals name;
    }
    proposal name {
      authentication-algorithm (md5 | sha-256 | sha1);
      authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
      description text;
      dh-group (group1 | group2 | group5 | group14);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      lifetime-seconds seconds;
    }
  }
  ipsec proposal name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description text;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
  }
  traceoptions {
    file {
      files number;
      match regexp;
      (no-world-readable | world-readable);
      size size;
    }
    flag {
      all | certificates | config | database | general | high-availability | ike
      | next-hop-tunnels | parse | policy-manager | routing-socket | thread | timer
    }
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security group-vpn]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure group VPN server. You configure the following on the group server:

- Phase 1 IKE SA for group members
- Phase 2 IPsec proposal
- Group identifier, group members, server-member communications, and group policies to be downloaded to members
- Group VPN trace options

 Copyright © 2011, Juniper Networks, Inc.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

service (AppDDoS)

Syntax
```
service <dns | http>;
```

Hierarchy Level [edit security idp application-ddos *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Defines the Application Layer service to be monitored for application-level DDoS attacks, such as DNS or HTTP.

Options ***service-name***—Name of the application layer protocol in lower case.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

service (Anomaly Attack)

Syntax
```
service service-name ;
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type anomaly]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Service is the protocol whose anomaly is defined in the attack. IP, TCP, UDP, and ICMP are also valid as services. (Protocol names must be entered in lower case.)

Options ***service-name***—Name of the protocol in lower case.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

service (Dynamic Attack Group)

Syntax

```
service {
  values [list-of-values];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a service filter to add attack objects based on the attack service, such as FTP, HTTP, NetBios, and so on.

Options **values**—Name of the service filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

service (Security IPsec)

Syntax service *service-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike proxy-identity]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the service (port and protocol combination) to protect.

Options *service-name* —Name of the service, as defined with **system-services** (**Interface Host-Inbound Traffic**) and **system-services** (**Zone Host-Inbound Traffic**).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- **system-services (Interface Host-Inbound Traffic) on page 751**
- **system-services (Zone Host-Inbound Traffic) on page 753**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

session-update-interval

Syntax session-update-interval *number*;

Hierarchy Level [edit security application-tracking]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the interval between session update messages for long-lived sessions being monitored by AppTrack. Byte count, packet count, and start and end times are updated and logged when the amount of time between session start or the previous update and the current time exceeds the interval.

Options ***number***—Minutes between updates.

Default: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

severity (Custom Attack)

Syntax severity (critical | info | major | minor | warning);

Hierarchy Level [edit security idp custom-attack *attack-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Select the severity that matches the lethality of the attack object on your network.

Options You can set the severity level to the following levels:

- **critical**—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges.
- **info**—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and Peer-to-Peer (P2P) parameters. You can use informational attack objects to obtain information about your network.
- **major**—Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device.
- **minor**—Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks.
- **warning**—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

severity (Dynamic Attack Group)

Syntax

```
severity {
   values [critical | info | major | minor | warning];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify a severity filter to add attack objects based on the attack severity.

Options **values**—Name of the severity filter. You can select from the following severity:

- **critical**—The attack is a critical one.
- **info**—Provide information of attack when it matches.
- **major**—The attack is a major one.
- **minor**—The attack is a minor one.
- **warning**—Issue a warning when attack matches.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

severity (IPS Rulebase)

Syntax severity (critical | info | major | minor | warning);

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set the rule severity levels in logging to support better organization and presentation of log records on the log server. You can use the default severity settings of the selected attack object, or choose a specific severity for your rule. The severity you configure in the rules overrides the inherited attack severity.

Options You can set the severity level to the following levels:

- **critical**—2
- **info**—3
- **major**—4
- **minor**—5
- **warning**—7

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

shellcode

Syntax shellcode (all | intel | no-shellcode | sparc);

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type anomaly]
[edit security idp custom-attack *attack-name* attack-type signature]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Shellcode signifies that the attack is a shellcode attack and is capable of creating its own shell.

Options **all**—All shellcode checks will be performed if this attack matches.

intel—Basic shellcode checks and Intel-specific shellcode checks will be performed.

no-shellcode—No shellcode checks will be performed.

sparc—Basic shellcode checks and Sparc-specific shellcode checks will be performed.

Default: Basic shellcode checks will be performed when this field is not configured.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

signature

Syntax

```
signature {
  context context-name ;
  direction (any | client-to-server | server-to-client);
  negate;
  pattern signature-pattern ;
  protocol {
    icmp {
      code {
        match (equal | greater-than | less-than | not-equal);
        value code-value ;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length ;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value ;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number ;
      }
      type {
        match (equal | greater-than | less-than | not-equal);
        value type-value ;
      }
    }
    ip {
      destination {
        match (equal | greater-than | less-than | not-equal);
        value hostname ;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value ;
      }
      ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
      }
      protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id ;
      }
      source {
        match (equal | greater-than | less-than | not-equal);
        value hostname ;
      }
      tos {
        match (equal | greater-than | less-than | not-equal);
```


Copyright © 2011, Juniper Networks, Inc.

```
        value type-of-service-in-decimal ;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram ;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live ;
      }
    }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number ;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length ;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port ;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length ;
      }
      mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size ;
      }
      option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option ;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number ;
      }
      source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port ;
      }
      tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
      }
      urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
```

```
            value urgent-pointer ;
          }
          window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor ;
          }
          window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size ;
          }
        }
        udp {
          data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length ;
          }
          destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port ;
          }
          source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port ;
          }
        }
      }
      protocol-binding {
        application application-name ;
        icmp;
        ip {
          protocol-number transport-layer-protocol-number ;
        }
        rpc {
          program-number rpc-program-number ;
        }
        tcp {
          minimum-port port-number maximum-port port-number ;
        }
        udp {
          minimum-port port-number maximum-port port-number ;
        }
      }
      regexp regular-expression ;
      shellcode (all | intel | no-shellcode | sparc);
    }
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description IDP uses stateful signatures to detect attacks. Stateful signatures are more specific than regular signatures. With stateful signatures, IDP can look for the specific protocol or service used to perpetrate the attack.

Options The remaining statements are explained separately.

 Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

sip

Syntax

```
sip {
  application-screen {
    protect {
      deny {
        all | destination-ip address ;
        timeout seconds ;
      }
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  c-timeout minutes ;
  disable;
  disable-call-id-hiding;
  inactive-media-timeout seconds ;
  maximum-call-duration minutes ;
  retain-hold-resource;
  t1-interval milliseconds ;
  t4-interval seconds ;
  traceoptions {
    flag {
      all <detail | extensive | terse>;
      call <detail | extensive | terse>;
      cc <detail | extensive | terse>;
      nat <detail | extensive | terse>;
      parser <detail | extensive | terse>;
      rm <detail | extensive | terse>;
    }
  }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the Session Initiation Protocol (SIP) ALG on the device.

Options **disable**—Disable the SIP ALG. By default, SIP ALG is enabled.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

smtp-profile (antispam utm-policy)

Syntax smtp-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-spam]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

smtp-profile (antivirus utm-policy)

Syntax smtp-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

smtp-profile (content-filtering utm-policy)

Syntax smtp-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sockets

Syntax sockets *value*;

Hierarchy Level [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter the number of sockets used for communicating between the client and server. The default is 1.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

sophos-engine

Syntax

```
sophos-engine {
    pattern-update {
      email-notify {
        admin–email email address;
        custom-message message;
        custom-message-subject message;
      }
      interval <minutes>;
      no-autoupdate;
      url  <url>;
      }
    }
    profile <name> {
      fallback-options {
        content-size (block | log-and-permit | permit);
        default (block | log-and-permit | permit);
        engine-not-ready (block | log-and-permit | permit);
        out-of-resource (block | log-and-permit | permit);
        timeout (block | log-and-permit | permit);
        too-many-requests (block | log-and-permit | permit);
      }
      notification-options {
        fallback-block {
          administrator-email email address;
          allow-email;
          custom-message message;
          custom-message-subject subject;
          display-host;
          no-notify-mail-sender;
          notify-mail-sender;
          type (message | protocol-only);
        }
        fallback-non-block {
          custom-message message;
          custom-message-subject subject;
          no-notify-mail-recipient;
          notify-mail-recipient;
        }
        virus-detection {
          custom-message message;
          custom-message-subject subject;
          no-notify-mail-sender;
          notify-mail-sender;
          type (protocol-only | message );
        }
      }
      scan-options {
        content-size-limit value;
        no-uri-check;
        timeout minutes;
        uri-check;
      }
```

```
        trickling {
            timeout value;
        }
    }
    sxl-timeout seconds;
    sxl-retry value;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the UTM Sophos antivirus feature.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source (IP Headers in Signature Attack)

Syntax

```
source {
    match (equal | greater-than | less-than | not-equal);
    value hostname ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the IP address of the attacking device.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***host-name*** —Match an ip-address or a host name.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

source (Source NAT)

Syntax

```
source {
  address-persistent;
  interface {
    port-overloading { off };
  }
  pool pool-name {
    address ip-address to ip-address ;
    host-address-base ip-address ;
    overflow-pool (interface | pool-name );
    port no-translation | range high ip-address low ip-address ;
    routing-instance routing-instance-name ;
  }
  pool-utilization-alarm {
    clear-threshold threshold-value ;
    raise-threshold threshold-value ;
  }
  port-randomization {
    disable;
  }
  rule-set rule-set-name {
    from interface [interface-name] |
    routing-instance [routing-instance-name] | zone [zone-name];
    rule rule-name {
      match {
        destination-address [destination-address];
        destination-port [range low ip-address high ip-address ]
        source-address [source-address];
      }
      then {
        source-nat (off | interface | pool pool-name );
        persistent-nat {
          address-mapping;
          inactivity-timeout seconds;
          max-session-number number;
          permit ( any-remote-host | target-host | target-host-port );
        }
      }
    }
    to interface [interface-name] |
    routing-instance [routing-instance-name] | zone [zone-name];
  }
}
```

Hierarchy Level [edit security nat]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure source NAT of the SRX Series device, which allows you to configure the following:

- Translate source IP address or addresses to the egress interface' IP address.

- Translate a range of source IP addresses to another range of IP addresses. This mapping is dynamic and without PAT.
- Translate a range of source IP addresses to another range of IP addresses. This mapping is dynamic and with PAT.
- Translate a range of source IP addresses to another range of IP addresses. This mapping is one-to-one, static, and without PAT.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (Destination NAT)

Syntax source-address [source-address];

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify source address to match the rule. You can configure multiple addresses or subnets.

Options ***source-address*** —Source address or a subnet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

source-address (IDP Policy)

Syntax source-address [address-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Junos 10.0.

Description Specify a source IP address or IP address set object to be used as the match source address object. The default value is any.

Options ***address-name*** —IP address, IP address set object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (IDP Sensor Configuration)

Syntax source-address *ip-address*;

Hierarchy Level [edit security idp sensor-configuration packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the source IP address for the carrier UDP packet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (Source NAT)

Syntax source-address [source-address];

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify source address to match the rule. You can configure multiple addresses or subnets.

Options ***source-address*** —Source address or a subnet.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-address (Security Policies)

Syntax
```
source-address {
  address-name ;
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

Options ***address-name*** —IP addresses, address sets, or wildcard addresses (represented as A.B.C.D/wildcard-mask).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

source-except

Syntax source-except [address-name];

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify a source IP address or IP address set object to specify all source address objects except the specified address objects. The default value is any.

Options *address-name* —IP address, IP address set object.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-interface

Syntax source-interface *interface-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* vpn-monitor]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the source interface for ICMP requests (VPN monitoring “hellos”). If no source interface is specified, the device automatically uses the local tunnel endpoint interface. (This statement is not supported on dynamic VPN implementations.)

Options *interface-name* —Name of the interface for the ICMP requests.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

source-ip-based

Syntax source-ip-based *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* limit-session]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Limit the number of concurrent sessions the device can initiate from a single source IP address.

Options ***number*** —Maximum number of concurrent sessions that can be initiated from a source IP address.

Range: 1 through 50000

Default: 128

NOTE: For SRX Series devices the applicable range is 1 through 8000000.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

source-nat

Syntax

```
source-nat (off | interface | pool pool-name);
  persistent-nat {
    address-mapping;
    inactivity-timeout seconds;
    max-session-number number;
    permit ( any-remote-host | target-host | target-host-port );
  }
```

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name* then]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the action of the source NAT rule.

Options

off — Do not perform the source NAT operation.

interface — Use egress interface IP address to perform the source NAT.

pool — Use user-defined source NAT pool to perform the source NAT.

The remaining statements are explained separately.

Required Privilege Level security — To view this statement in the configuration.
security-contro l— To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

source-port

Syntax

```
source-port {
   match (equal | greater-than | less-than | not-equal);
   value source-port;
}
```

Hierarchy Level

[edit security idp custom-attack ***attack-name*** attack-type signature protocol udp]
[edit security idp custom-attack ***attack-name*** attack-type signature protocol tcp]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify the port number on the attacking device.

Options

match (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***source-port***—Port number on the attacking device.

Range: 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

source-threshold

Syntax source-threshold *number* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Specify the number of SYN segments that the device can receive per second from a single source IP address (regardless of the destination IP address and port number) before the device begins dropping connection requests from that source.

Options *number* —Number of SYN segments to be received per second before the device starts dropping connection requests.

Range: 4 through 100,000 per second

Default: 1024 per second

NOTE: For SRX Series devices the applicable range is 4 through 1,000,000 per second.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

spam-action

Syntax spam-action (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-spam sbl profile *profile-name* sbl-default-server]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the action to be taken by the device when spam is detected.

Options
- block— Block e-mail
- tag-header—Tag header of e-mail
- tag-subject—Tag subject of e-mail

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

spi

Syntax spi *spi-value* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* manual]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure a security parameter index (SPI) for a security association (SA). (This statement is not supported on dynamic VPN implementations.)

Options ***spi-value*** —An arbitrary value that uniquely identifies which security association (SA) to use at the receiving host (the destination address in the packet).

Range: 256 through 16639

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

sql

Syntax

```
sql {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the Oracle SQL ALG on the device.

Options

disable—Disable the SQL ALG. By default, the SQL ALG is enabled.

traceoptions—Configure SQL ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

ssh-known-hosts

Syntax

```
ssh-known-hosts {
   fetch-from-server fetch-from-server ;
   host hostname {
      dsa-key base64-encoded-dsa-key ;
      rsa-key base64-encoded-dsa-key ;
      rsa1-key base64-encoded-dsa-key ;
   }
   load-key-file key-file ;
}
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure SSH support for known hosts and for administering SSH host key updates.

Options

dsa-key—Digital signature algorithm (DSA) for SSH version 2.

fetch-from-server—Retrieve SSH public host key information from a specified server.

load-key-file—Import SSH host key information from the **/var/tmp/ssh-known-hosts** file.

rsa-key—Public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.

rsa1-key—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

ssl-inspection

Syntax

```
ssl-inspection {
   sessions number ;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Inspect HTTP traffic encrypted in SSL protocol. SSL inspection is disabled by default. It is enabled if you configure ssl-inspection.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

start-log

Syntax

```
start-log value ;
```

Hierarchy Level [edit security idp sensor-configuration log suppression]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify how many instances of a specific event must occur before log suppression begins.

Options *value* —Log suppression begins after how many occurrences.

Range: 1 through 128

Default: 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

start-time

Syntax start-time *start-time* ;

Hierarchy Level [edit security idp security-package automatic]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the time that the device automatically starts downloading the updated signature database from the specified URL.

Options *start-time* —Time in MM-DD.hh:mm format.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

static

Syntax

```
static {
  rule-set rule-set-name {
    from interface [interface-name] |
    routing-instance [routing-instance-name] | zone [zone-name];
    rule rule-name {
      match {
        destination-address [destination-address];
      }
      then {
        static-nat prefix < addr-prefix >
        <routing-instance routing-instance-name >;
      }
    }
  }
}
```

Hierarchy Level [edit security nat]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Configure static NAT of SRX Series device.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

static-nat

Syntax static-nat prefix < *addr-prefix* > <routing-instance *routing-instance-name* >;

Hierarchy Level [edit security nat static rule-set *rule-set-name* rule *rule-name* then]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the translated address of the static NAT rule.

Options ***address-prefix*** —Static IP address prefix.

routing-instance ***routing-instance-name*** —Use user-defined static NAT routing-instance to perform static NAT. By default, the **routing-instance** is the same as the **from routing-instance**.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

statistics

Syntax statistics interval <*minutes*>;

Hierarchy Level [edit security idp sensor-configuration application-ddos]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description The statistics command will enable application-level DDoS statistic collection at the defined internal. Statistic report files are stored on the routing engine (RE) data storage device in /var/log/addos in comma separated value (CSV) format. The data storage device must have at least 2GB of free space before logging will occur.

Options ***minutes*** —Set the interval in minutes that will define when application statistic will be collected.

Range: 1 through 60 minutes (1 minute increments)

Default: 1 minute

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

strict-syn-check

Syntax strict-syn-check

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Enable the strict three-way handshake check for the TCP session. It enhances security by dropping data packets before the three-way handshake is done. By default, strict-syn-check is disabled.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sunrpc

Syntax

```
sunrpc {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 9.0 of Junos OS.

Description Specify the Sun Microsystems remote procedure call (RPC) ALG on the device.

Options **disable**—Disable the Sun RPC ALG. By default, the Sun RPC ALG is enabled.

traceoptions—Configure the Sun RPC ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- **all**—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

suppression

Syntax

```
suppression {
   disable;
   include-destination-address;
   max-logs-operate value ;
   max-time-report value ;
   start-log value ;
}
```

Hierarchy Level [edit security idp sensor-configuration log]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Log suppression reduces the number of logs by displaying a single record for multiple occurrences of the same event. Log suppression can negatively impact sensor performance if the reporting interval is set too high. By default this feature is enabled.

Options **disable**—Disable log suppression.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

surf-control-integrated

Syntax

```
surf-control-integrated {
cache {
   timeout value;
   }
   server {
   host host-name;
      port number;
   }
profile profile-name{
   default (log-and-permit | block);
      custom-block-message value;
      fallback-settings {
      default (log-and-permit | block);
         server-connectivity (log-and-permit | block);
         timeout (log-and-permit | block);
         too-many-requests (log-and-permit | block);
      }
      category customurl-list name {
      action (log-and-permit | block);
      }
   }
```

Hierarchy Level [set security utm feature-profile web-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure the UTM web-filtering integrated feature.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

sxl-retry

Syntax sxl-retry *value;*

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

Options ***value*** —Number of retries.
Range: 0 through 5
Default: 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

sxl-timeout

Syntax sxl-timeout *seconds;*

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure the timeout value for responses to a Sophos checksum or URI query.

Options ***seconds*** —Number of seconds before timeout occurs.
Range: 1 through 5 seconds
Default: 2 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

syn-ack-ack-proxy

Syntax

```
syn-ack-ack-proxy; {
   threshold number ,
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.

Description Prevent the SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. This behavior consumes all open slots, generating a denial-of-service (DoS) condition.

Options threshold *number* — Number of connections from any single IP address.

Range: 1 through 250000

Default: 512

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

syn-fin

Syntax syn-fin;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of an illegal combination of flags that attackers can use to consume sessions on the target device, thus resulting in a denial-of-service (DoS) condition.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

syn-flood

Syntax

```
syn-flood {
   alarm-threshold number ;
   attack-threshold number ;
   destination-threshold number ;
   source-threshold number ;
   timeout seconds ;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure detection and prevention of SYN flood attacks. Such attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

syn-flood-protection-mode

Syntax syn-flood-protection-mode (syn-cookie | syn-proxy);

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.

Description Enable SYN cookie or SYN proxy defenses against SYN attacks. SYN flood protection mode is enabled globally on the device and is activated when the configured **syn-flood attack-threshold value** is exceeded.

Options **syn-cookie**—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default.

syn-proxy—Uses a proxy to handle the SYN attack.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- **attack-threshold on page 351**
- *Junos OS Security Configuration Guide*

syn-frag

Syntax syn-frag;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of a SYN fragment attack and drops any packet fragments used for the attack. A SYN fragment attack floods the target host with SYN packet fragments. The host caches these fragments, waiting for the remaining fragments to arrive so it can reassemble them. The flood of connections that cannot be completed eventually fills the host's memory buffer. No further connections are possible, and damage to the host's operating system can occur.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

system-services (Interface Host-Inbound Traffic)

Syntax

```
system-services {
  service-name ;
  service-name <except>;
}
```

Hierarchy Level

[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the types of traffic that can reach the device on a particular interface.

Options

service-name —Service for which traffic is allowed. The following services are supported:

- **all**—Enable all possible system services available on the Routing Engine (RE).
- **any-service**—Enable services on entire port range.
- **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
- **dhcp**—Enable incoming DHCP requests.
- **dns**—Enable incoming DNS services.
- **finger**—Enable incoming finger traffic.
- **ftp**—Enable incoming FTP traffic.
- **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
- **http**—Enable incoming J-Web or clear-text Web authentication traffic.
- **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
- **ike**—Enable Internet Key Exchange traffic.
- **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
- **ping**—Allow the device to respond to ICMP echo requests.
- **rlogin**—Enable incoming **rlogin** (remote login) traffic.
- **rpm**—Enable incoming real-time performance monitoring (RPM) traffic.
- **rsh**—Enable incoming Remote Shell (**rsh**) traffic.
- **snmp**—Enable incoming SNMP traffic (UDP port 161).
- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).
- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.

Copyright © 2011, Juniper Networks, Inc.

- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.

except—(Optional) except can only be used if all has been defined.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

system-services (Zone Host-Inbound Traffic)

Syntax

```
system-services {
   service-name ;
   service-name  <except>;
}
```

Hierarchy Level [edit security zones security-zone *zone-name* host-inbound-traffic]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the types of traffic that can reach the device for all interfaces in a zone.

Options *service-name* —Service for which traffic is allowed. The following services are supported:

- **all**—Enable all possible system services available on the Routing Engine (RE).
- **any-service**—Enable services on entire port range.
- **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
- **dhcp**—Enable incoming DHCP requests.
- **dns**—Enable incoming DNS services.
- **finger**—Enable incoming finger traffic.
- **ftp**—Enable incoming FTP traffic.
- **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
- **http**—Enable incoming J-Web or clear-text Web authentication traffic.
- **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
- **ike**—Enable Internet Key Exchange traffic.
- **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
- **ping**—Allow the device to respond to ICMP echo requests.
- **rlogin**—Enable incoming **rlogin** (remote login) traffic.
- **rpm**—Enable incoming Real-time performance monitoring (RPM) traffic.
- **rsh**—Enable incoming Remote Shell (**rsh**) traffic.
- **snmp**—Enable incoming SNMP traffic (UDP port 161).
- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).
- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.
- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).

Copyright © 2011, Juniper Networks, Inc.

- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.

except—(Optional) except can only be used if all has been defined.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

t1-interval

Syntax t1-interval ***milliseconds*** ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum round-trip time (RTT) (in milliseconds) allowed for Session Initiation Protocol (SIP) transactions.

Options ***milliseconds*** —Maximum round-trip time (RTT) allowed measured in milliseconds.

Range: 500 through 5000 milliseconds

Default: 500 milliseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

t4-interval

Syntax t4-interval *seconds* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum length of time (in seconds) that the network can take to clear messages between client and server Session Initiation Protocol (SIP) transactions.

Options ***seconds*** —Maximum number of seconds that the network can take to clear messages between client and server transactions.

Range: 5 through 10 seconds

Default: 5 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

talk

Syntax

```
talk {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the TALK program ALG on the device.

Options

disable—Disable the TALK program ALG. By default, the TALK program ALG is enabled.

traceoptions—Configure TALK program ALG tracing options.

flag—Trace operation to perform. To perform more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

target

Syntax target (destination-address | service | source-address | source-zone | zone-service);

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the blocking options that you want to set to block the future connections. Blocking options can be based on the following matches of the attack traffic:

Options

- **destination-address**—Matches traffic based on the destination address of the attack traffic.
- **service**—For TCP and UDP, matches traffic based on the source address, source port, destination address, and destination port of the attack traffic. This is the default.

  For ICMP flows, the destination port is 0. Any ICMP flow matching source port, source address, and destination address is blocked.
- **source-address**—Matches traffic based on the source address of the attack traffic.
- **source-zone**—Matches traffic based on the source zone of the attack traffic.
- **zone-service**—Matches traffic based on the source zone, destination address, destination port, and protocol of the attack traffic.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

tcp (Protocol Binding Custom Attack)

Syntax

```
tcp {
   minimum-port port-number maximum-port port-number;
}
```

Hierarchy Level

[edit security idp custom-attack ***attack-name*** attack-type chain protocol-binding]
[edit security idp custom-attack ***attack-name*** attack-type signature protocol-binding]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Allow IDP to match the attack for specified TCP port(s).

Options

minimum-port ***port-number***—Minimum port in the port range.

Range: 0 through 65,535

maximum-port***port-number***—Maximum port in the port range.

Range: 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tcp (Security Screen)

Syntax

```
tcp {
   fin-no-ack;
   land;
   port-scan {
      threshold number ;
   }
   syn-ack-ack-proxy {
      threshold number ;
   }
   syn-fin;
   syn-flood {
      alarm-threshold number ;
      attack-threshold number ;
      destination-threshold number ;
      source-threshold number ;
      timeout seconds ;
   }
   syn-frag;
   tcp-no-flag;
   tcp-sweep {
      threshold threshold number;
   }
   winnuke;
}
```

Hierarchy Level

[edit security screen ids-option *screen-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure TCP-layer intrusion detection service (IDS) options.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

tcp (Signature Attack)

Syntax

```
tcp {
  ack-number {
    match (equal | greater-than | less-than | not-equal);
    value acknowledgement-number ;
  }
  data-length {
    match (equal | greater-than | less-than | not-equal);
    value tcp-data-length ;
  }
  destination-port {
    match (equal | greater-than | less-than | not-equal);
    value destination-port ;
  }
  header-length {
    match (equal | greater-than | less-than | not-equal);
    value header-length ;
  }
  mss {
    match (equal | greater-than | less-than | not-equal);
    value maximum-segment-size ;
  }
  option {
    match (equal | greater-than | less-than | not-equal);
    value tcp-option ;
  }
  sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number ;
  }
  source-port {
    match (equal | greater-than | less-than | not-equal);
    value source-port ;
  }
  tcp-flags {
    (ack | no-ack);
    (fin | no-fin);
    (psh | no-psh);
    (r1 | no-r1);
    (r2 | no-r2);
    (rst | no-rst);
    (syn | no-syn);
    (urg | no-urg);
  }
  urgent-pointer {
    match (equal | greater-than | less-than | not-equal);
    value urgent-pointer ;
  }
  window-scale {
    match (equal | greater-than | less-than | not-equal);
    value window-scale-factor ;
  }
  window-size {
```


Copyright © 2011, Juniper Networks, Inc.

```
        match (equal | greater-than | less-than | not-equal);
        value window-size ;
    }
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to match the TCP header information for the signature attack.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

tcp-flags

Syntax

```
tcp-flags {
   (ack | no-ack);
   (fin | no-fin);
   (psh | no-psh);
   (r1 | no-r1);
   (r2 | no-r2);
   (rst | no-rst);
   (syn | no-syn);
   (urg | no-urg);
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Specify that IDP looks for a pattern match whether or not the TCP flag is set.

Options

ack | **no-ack**—When set, the acknowledgment flag acknowledges receipt of a packet.

fin | **no-fin**—When set, the final flag indicates that the packet transfer is complete and the connection can be closed.

psh | **no-psh**—When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.

r1 | **no-r1**—When set, indicates that the R1 retransmission threshold has been reached.

r2 | **no-r2**—When set, indicates that the R2 retransmission threshold has been reached.

rst | **no-rst**—When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.

syn | **no-syn**—When set, indicates that the sending device is asking for a three-way handshake to initialize communications.

urg | **no-urg**—When set, the urgent flag indicates that the packet data is urgent.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tcp-initial-timeout

Syntax tcp-initial-timeout *seconds* ;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Define the length of time (in seconds) that the device keeps an initial TCP session in the session table before dropping it, or until the device receives a FIN (no more data) or RST (reset) packet.

Options ***seconds*** —Number of seconds that the device keeps an initial TCP session in the session table before dropping it.

Range: 20 through 300 seconds

Default: 20 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

tcp-mss

Syntax

```
tcp-mss {
  all-tcp {
    mss value ;
  }
  gre-in {
    mss value ;
  }
  gre-out {
    mss value ;
  }
  ipsec-vpn {
    mss value ;
  }
}
```

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure TCP maximum segment size (TCP MSS) for the following packet types:

- All TCP packets for network traffic.
- GRE packets entering the IPsec VPN tunnel.
- GRE packets exiting the IPsec VPN tunnel.
- TCP packets entering the IPsec VPN tunnel.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tcp-no-flag

Syntax tcp-no-flag;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to drop illegal TCP packets with a missing or malformed flag field.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tcp-rst

Syntax tcp-rst;

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable the device to send a TCP segment with the RST (reset) flag set to 1 (one) in response to a TCP segment with any flag other than SYN set and that does not belong to an existing session.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tcp-session

Syntax

```
tcp-session {
   no-sequence-check;
   no-syn-check;
   no-syn-check-in-tunnel;
   rst-invalidate-session;
   rst-sequence-check;
   tcp-initial-timeout seconds ;
}
```

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure TCP session attributes:

- TCP sequence number checking.
- TCP SYN bit checking.
- Reset (RST) checking.
- Initial TCP session timeout.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tcp-sweep

Syntax

```
tcp-sweep {
   threshold number;
}
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the device to detect and prevent TCP sweep attack. In a TCP sweep attack, an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further TCP packets from that host for the remainder of the specified threshold period.

Options **threshold** *number*—Maximum number of microseconds during which up to 10 TCP SYN packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers TCP Sweep attack response on the router during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

terminal

Syntax

```
terminal;
```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Set or unset a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

test

Syntax test *test-condition* ;}

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type anomaly]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify protocol anomaly condition to be checked.

Options *test-condition* —Name of the anomaly test condition.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tftp

Syntax

```
tftp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of Junos OS.

Description Configure the Trivial File Transfer Protocol (TFTP) ALG on the device.

Options **disable**—Disable the TFTP ALG. By default, the TFTP ALG is enabled.

NOTE: By default, the TFTP ALG is disabled for SRX Series devices.

traceoptions—Configure TFTP ALG tracing options.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

all—Trace all events.

extensive—(Optional) Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

then (Application Firewall)

Syntax

```
then {
   permit | deny;
}
```

Hierarchy Level [edit security application-firewall rule-set *rule-set-name* rule *rule-name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Specify the action to be performed when traffic matches the specified application firewall rule.

Options ***permit***—Permit traffic that matches the rule.

deny—Deny the traffic. Packets are dropped.

Usage Guidelines For configuration instructions and examples, see the *Junos OS Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

then (Destination NAT)

Syntax

```
then {
   destination-nat (off | pool pool-name );
}
```

Hierarchy Level [edit security nat destination rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the action to be performed when traffic matches the destination NAT rule criteria.

Options The remaining statement is explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

then (IDP Policy)

Syntax

```
then {
  action {
    <close-client | close-client-and-server | close-server |
    drop-connection | drop-packet | ignore-connection |
    mark-diffserv value | no-action | recommended>;
  }
  ip-action {
    <ip-block | ip-close | ip-notify>;
    log;
    target <destination-address | service | source-address |
    source-zone | zone-service>;
    timeout seconds ;
  }
  notification {
    log-attacks {
      alert;
    }
    packet-log {
      pre-attack number;
      post-attack number;
      post-attack-timeout seconds;
    }
  }
  severity <critical | info | major | minor | warning>;
}
```

Hierarchy Level

[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

Release Information

Statement introduced in Release 9.2 of Junos OS.

Description

Specify the action to be performed when traffic matches the defined criteria.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

then (rulebase-ddos)

Syntax

```
then {
   action <close-server | drop-connection | drop-packet | no-action>;
   ip-action {
      <ip-block | ip-close | ip-notify>
      timeout secconds;
   }
}
```

Hierarchy Level [edit security idp idp-policy ***policy-name*** rulebase-ddos rule ***rule-name***]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Specify the session action to be performed when traffic matches the defined criteria.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

then (Security Policies)

Syntax

```
then {
  count {
    alarm {
      per-minute-threshold number;
      per-second-threshold number ;
    }
  }
  (deny | reject);
  permit {
    application-services (redirect-wx | reverse-redirect-wx);
    destination-address {
      drop-translated;
      drop-untranslated;
    }
    firewall-authentication {
      pass-through {
        access-profile profile-name ;
        client-match match-name ;
        web-redirect;
      }
      web-authentication {
        client-match user-or-group ;
      }
    }
    tunnel {
      ipsec-group-vpn group-vpn;
      ipsec-vpn vpn-name ;
      pair-policy pair-policy ;
    }
  }
  log {
    session-close;
    session-init;
  }
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the policy action to be performed when packets match the defined criteria.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

then (Source NAT)

Syntax

```
then {
  source-nat (off | interface | pool pool-name );
  persistent-nat {
    address-mapping;
    inactivity-timeout seconds;
    max-session-number number;
    permit ( any-remote-host | target-host | target-host-port );
  }
}
```

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the action to be performed when traffic matches the source NAT rule criteria.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

then (Static NAT)

Syntax

```
then {
  static-nat prefix < addr-prefix > <routing-instance routing-instance-name >;
}
```

Hierarchy Level [edit security nat static rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Specify the action to be performed when traffic matches the static NAT rule criteria.

Options The remaining statement is explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

threshold

Syntax threshold *number* ;

Hierarchy Level [edit security ike gateway *gateway-name* dead-peer-detection]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. (This statement is not supported on dynamic VPN implementations.)

Options *number* —Maximum number of unsuccessful DPD requests to be sent.

Range: 1 through 5

Output: 5

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

time-binding

Syntax

```
time-binding {
   count count-value ;
   scope (destination | peer | source);
}
```

Hierarchy Level [edit security idp custom-attack *attack-name*]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Allow IDP to detect a sequence of the same attacks over a period of time.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

time-binding-count

Syntax

```
context <context-name> {
   time-binding-count number;
}
```

Hierarchy Level [edit security idp application–ddos *name* **context** *context-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description (Optional) Configure the number of context or context value hits from each client over the time binding period to determine if it should be considered a bot client.

Options *number* —Time-binding count for the source address.

Range: 2 to 50,000

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

time-binding-period statement

Syntax

```
context <context-name> {
   time-binding-period seconds;
}
```

Hierarchy Level [edit security idp application-ddos *name* context *context-name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description (Optional) Configure the time-binding period to determine if a client should be classified as a bot client or not. This setting is used in conjunction with time-binding count to detect an attack if a client request for the same context value exceeds time-binding-count times in time-binding-period seconds.

Contexts values are monitored until overall requests for a given application-level distributed denial-of-service (DDoS) application no longer exceeds hit-rate-threshold limit for each configured context. If overall context requests exceeds hit-rate-threshold limit, context value monitoring is disabled and system applies time-binding with PEER scope (source-ip, destination-ip, destination-port, destination-protocol, destination-zone), if configured.

Options *number*—Time-binding period (seconds).

Range: 1 to 3600 seconds

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

timeout (GTP)

Syntax timeout;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Sets the tunnel timeout value in hours. The default is 24 hours. Via the process of stateful inspection, if a device detects no activity in a tunnel for a specified period of time (timeout), it removes the tunnel from the state table. The time out range is 1 through 1,000 hours.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

timeout (IDP Policy)

Syntax timeout *seconds* ;

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the number of seconds that you want the IP action to remain in effect after a traffic match.

Options *seconds* —Number of seconds the IP action should remain effective.
Range: 0 through 65,535 seconds
Default: 0 second

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

timeout (Security Screen)

Syntax timeout *seconds* ;

Hierarchy Level [edit security screen ids-option *screen-name* tcp syn-flood]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.

Options *seconds* —Time interval before a half-completed connection is dropped from the queue.

Range: 1 through 50 seconds

Default: 20 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

timeout (antivirus fallback-options)

Syntax timeout (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information Statement introduced in Release 9.5 of Junos OS. Updated in

Description Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option. The default action is BLOCK.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

timeout (antivirus scan-options)

Syntax timeout *value*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* scan-options]

Release Information Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

Description The scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

timeout (web-filtering surf-control-integrated cache)

Syntax timeout *value*;

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated cache]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Set the cache timeout parameters for surf-control-integrated web filtering (24 hours is the default and the maximum allowed life span of cached items) for J Series devices and SRX Series devices.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

timeout (web-filtering fallback-settings)

Syntax timeout (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Fallback settings tell the system how to handle errors.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

timeout (web-filtering websense-redirect profile)

Syntax timeout *value*;

Hierarchy Level [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 10 seconds.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

to

Syntax
to interface [interface-name] |
routing-instance [routing-instance-name] | zone [zone-name];

Hierarchy Level
[edit security nat source rule-set *rule-set-name*]

Release Information
Statement introduced in Release 9.2 of Junos OS.

Description
Specify the destination of the packet among the routing instance, interface, or zone.

Options
interface *interface-name* —Name of the interface.

routing-instance *routing-instance-name* —Name of the routing instance.

zone *zone-name* —Name of the zone.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

to-zone

Syntax
to-zone *zone-name* ;

Hierarchy Level
[edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

Release Information
Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

Description
Specify a destination zone to be associated with the security policy. The default value is any.

Options
zone-name —Name of the destination zone object.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

too-many-requests (antivirus fallback-options)

Syntax too-many-requests (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* fallback-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

too-many-requests (web-filtering fallback-settings)

Syntax too-many-requests (log-and-permit | block);

Hierarchy Level [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

tos

Syntax

```
tos {
  match (equal | greater-than | less-than | not-equal);
  value type-of-service-in-decimal ;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the type of service.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***type-of-service-in-decimal*** —The following service types are available:

- 0000—Default
- 0001—Minimize Cost
- 0002—Maximize Reliability
- 0003—Maximize Throughput
- 0004—Minimize Delay
- 0005—Maximize Security

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

total-length

Syntax

```
total-length {
  match (equal | greater-than | less-than | not-equal);
  value total-length-of-ip-datagram;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the number of bytes in the packet, including all header fields and the data payload.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***total-length-of-ip-datagram*** —Length of the IP datagram.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

total-memory

Syntax total-memory *percentage*;

Hierarchy Level [edit security idp sensor-configuration packet-log]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the maximum amount of memory to be allocated to packet capture for the device. This value is expressed as a percentage of the memory available on the device. The total memory for a device will differ depending on its operating mode.

Options *percentage*—Amount of packet capture memory expressed as a percentage of total memory for the device mode.

Range: 1 to 100 percent

Default: 10

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

traceoptions (Application Firewall)

Syntax

```
traceoptions {
  file filename {
    <files number>;
    <match regular-expression>;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag {
    all;
    compilation;
    configuration;
    ipc;
    lookup;
  }
  no-remote-trace;
}
```

Hierarchy Level [edit security application-firewall]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure trace options for the application firewall.

Options

- **file** ***filename***—Name of the file to which to write the trace information
- **files** ***number***—Specify the maximum number of trace files

  Range: 2 through 1000 files
- **match** ***regular-expression***—Regular expression for lines to be logged
- **size** ***maximum-file-size***—Maximum trace file size

  Range: 10,240 to 1,073,741,824 bytes
- **no-world-readable**—Do not allow any user to read the log file
- **world-readable**—Allow any user to read the log file

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- **all**—Trace all
- **compilation**—Trace rule set compilation events
- **configuration**—Trace configuration events
- **ipc**—Trace process inter communication events
- **lookup**—Trace rule set lookup events

no-remote-trace—Set remote tracing as disabled

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (firewall-authentication)

Syntax

```
traceoptions {
  flag {
    all <detail | extensive | terse>;
    authentication <detail | extensive | terse>;
    proxy <detail | extensive | terse>;
  }
}
```

Hierarchy Level
[edit security firewall-authentication]

Release Information
Statement introduced in Release 8.5 of Junos OS.

Description
Define data-plane firewall authentication tracing options.

Options
flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Enable all tracing operations
- **authentication**—Trace data-plane firewall authentication events
- **proxy**—Trace data-plane firewall authentication proxy events

detail—Display moderate amount of data in trace.

extensive—Display extensive amount of data in trace.

terse—Display minimum amount of data in trace.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (H.323 ALG)

Syntax

```
traceoptions {
  flag {
    all <detail | extensive | terse>;
    cc <detail | extensive | terse>;
    h225-asn1 <detail | extensive | terse>;
    h245 <detail | extensive | terse>;
    h245-asn1 <detail | extensive | terse>;
    q931 <detail | extensive | terse>;
    ras <detail | extensive | terse>;
    ras-asn1 <detail | extensive | terse>;
  }
}
```

Hierarchy Level [edit security alg h323]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure H.323 tracing options.

Options flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **cc**—Trace chassis cluster functions
- **h225-asn1**—Trace H.225 ASN.1 processing activity
- **h245**—Trace H.245 processing activity
- **h245-asn1**—Trace H.245 ASN.1 processing activity
- **q931**—Trace Q.931 processing activity
- **ras**—Trace remote access server (RAS) processing activity
- **ras-asn1**—Trace RAS ASN.1 processing activity

detail—Display moderate amount of data in trace.

extensive—Display extensive amount of data in trace.

terse—Display minimum amount of data in trace.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

traceoptions (Flow)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression> <size maximum-file-size>
  <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure flow tracing options.

Options

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number* —(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0**, then *trace-file.1*, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **ager**—Trace session ageout related events
- **all**—Trace with all flags enabled
- **basic-datapath**—Trace basic packet flow activity
- **cli**—Trace CLI configuration activity and command changes
- **errors**—Trace flow errors activity
- **fragmentation**—Trace IP fragmentation and reassembly events
- **chassis-cluster**—Trace chassis cluster information
- **host-traffic**—Trace host traffic information
- **lookup**—Trace lookup events
- **multicast**—Trace multicast flow information
- **packet-drops**—Trace packet drop activity
- **route**—Trace route information
- **session**—Trace session creation and deletion events
- **session-scan**—Trace session scan information
- **tcp-advanced**—Trace advanced TCP packet flow activity
- **tcp-basic**—Trace TCP packet flow activity
- **tunnel**—Trace tunnel information

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

traceoptions (firewall-authentication)

Syntax

```
traceoptions
  file filename {
    <files | match | no-world-readable | size | world-readable>;
    }
  flag {
    < all | chassis-cluster | configuration | flow | parser | >;
    }
  no-remote-trace;
```

Hierarchy Level [edit security gprs gtp]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable the device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification.

Options file

- **filename**—Name of the file in which to write trace information
- **files**—Maximum number of trace files with a range of 2 through 1,000
- **match**—Regular expression for lines to be logged
- **no-world-readable**—Do not allow any user to read the log file
- **size**—Maximum trace file size with a range of 10,240 to 1,073,741,824
- **world-readable**—Allow any user to read the log file

flag

- **all**—Trace everything
- **chassis-cluster**—Trace chassis cluster events
- **configuration**—Trace configuration events
- **flow**—Trace flow events
- **parsar**—Trace parser events

no-remote-trace—Set remote tracing as disabled

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (Group VPN)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
  no-remote-trace;
}
```

Hierarchy Level [edit security group-vpn server]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure group VPN trace options.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1*, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

Copyright © 2011, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all activity
- **certificates**—Trace certificate-related activity
- **database**—Trace SA-related database activity
- **general**—Trace general activity
- **high-availability**—Trace high-availability operations
- **ike**—Trace IKE protocol activity
- **next-hop-tunnels**—Trace next-hop tunnel operations
- **parse**—Trace configuration processing
- **policy-manager**—Trace IKE callback activity
- **routing-socket**—Trace routing socket activity
- **thread**—Trace thread processing
- **timer**—Trace timer activity

no-remote-trace—Disable remote tracing.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (IDP)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag all;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Configure IDP tracing options.

Options

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number* —(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

Copyright © 2011, Juniper Networks, Inc.

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all iked process modules activity

level—Set the level of debugging the output option.

- **all**—Match all levels
- **error**—Match error conditions
- **info**—Match informational messages
- **notice**—Match conditions that should be handled specially
- **verbose**—Match verbose messages
- **warning**—Match warning messages

no-remote-trace—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (IKE)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit security ike]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure IKE tracing options.

Options

file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number* —(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

 Copyright © 2011, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all iked process modules activity
- **certificates**—Trace certificate-related activity
- **database**—Trace VPN-related database activity
- **general**—Trace general activity
- **ike**—Trace IKE protocol activity
- **parse**—Trace VPN parsing activity
- **policy-manager**—Trace iked callback activity
- **routing-socket**—Trace routing socket activity
- **timer**—Trace timer activity
- **snmp**—Trace SNMP operations activity

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (IPsec)

Syntax

```
traceoptions {
  flag {
    all;
    next-hop-tunnel-binding;
    packet-drops;
    packet-processing;
    security-associations;
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure IPsec tracing options.

Options **flag**—To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **next-hop-tunnel-binding**—Trace next-hop tunnel binding events
- **packet-drops**—Trace packet drop activity
- **packet-processing**—Trace data packet processing events
- **security-associations**—Trace security association (SA) management events

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

traceoptions (MGCP ALG)

Syntax

```
traceoptions {
  flag {
    all <extensive>;
    call <extensive>;
    cc <extensive>;
    decode <extensive>;
    error <extensive>;
    nat <extensive>;
    packet <extensive>;
    rm <extensive>;
  }
}
```

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure Media Gateway Control Protocol (MGCP) tracing options.

Options flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **call**—Trace call processing activity
- **cc**—Trace chassis cluster functions
- **decode**—Trace decoder operations activity
- **error**—Trace processing errors activity
- **nat**—Trace Network Address Translation (NAT) processing activity
- **packet**—Trace MGCP protocol packet processing activity
- **rm**—Trace MGCP Resource Management (Resmgr) functions activity

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (NAT)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag {
    all;
    destination-nat-pfe;
    destination-nat-re;
    destination-nat-rt;
    source-nat-pfe;
    source-nat-re;
    source-nat-rt;
    static-nat-pfe;
    static-nat-re;
    static-nat-rt;
  }
  no-remote-trace;
}
```

Hierarchy Level [edit security nat]

Release Information Statement modified in Release 9.6 of Junos OS.

Description Configure NAT tracing options.

Options ***filename*** —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number*** —(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*** **.0,** then ***trace-file.1*** , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*** **.0**. When the **trace-file** again reaches its maximum size, ***trace-file*** **.0** is renamed ***trace-file*** **.1** and ***trace-file*** is renamed ***trace-file*** **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

 Copyright © 2011, Juniper Networks, Inc.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **destination-nat-pfe**—Trace destination NAT events on PFE-ukernel side
- **destination-nat-re**—Trace destination NAT events on Routing Engine (RE) side
- **destination-nat-rt**—Trace destination NAT events on Packet Forwarding Engine real-time (PFE-RT) side
- **source-nat-pfe**—Trace source NAT events on PFE-ukernel side
- **source-nat-re**—Trace source NAT events on RE side
- **source-nat-rt**—Trace source NAT events on PFE-RT side
- **static-nat-pfe**—Trace static NAT events on PFE-ukernel side
- **static-nat-re**—Trace static NAT events on RE side
- **static-nat-rt**—Trace static NAT events on PFE-RT side

no-remote-trace—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (datapath-debug)

Syntax **traceoptions;**

Hierarchy Level [edit security datapath-debug]

Release Information Command introduced in Release 9.6 of Junos OS.

Description Sets the trace options for datapath-debug.

Options ***apply-groups***—Groups from which to inherit configuration data.

apply-groups-except—Do not inherit configuration data from these groups.

file —Trace file information

no-remote-trace—Disable remote tracing

rate-limit—Limit the incoming rate of trace messages (0..4,294,967,295)

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

traceoptions (PKI)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit security pki]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure public key infrastructure (PKI) tracing options.

Options

filename —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number*** —(Optional) Specify the maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*** **.0,** then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*** **.0**. When the **trace-file** again reaches its maximum size, ***trace-file*** **.0** is renamed ***trace-file*** **.1** and ***trace-file*** is renamed ***trace-file*** **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **certificate-verification**—Trace PKI certificate verification events
- **online-crl-check**—Trace PKI online certificate revocation list (CRL) events

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (Policies)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit security policies]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure policy tracing options.

Options

filename —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number*** —(Optional) Specify the maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*** **.0,** then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*** **.0**. When the **trace-file** again reaches its maximum size, ***trace-file*** **.0** is renamed ***trace-file*** **.1** and ***trace-file*** is renamed ***trace-file*** **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **configuration**—Trace configuration events
- **compilation**—Trace policy compilation events
- **ipc**—Trace process inter communication events
- **lookup**—Trace policy lookup events
- **routing-socket**—Trace routing socket events
- **rules**—Trace policy rules-related events

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (SCCP ALG)

Syntax

```
traceoptions {
  flag {
    all <extensive>;
    call <extensive>;
    cc <extensive>;
    cli <extensive>;
    decode <extensive>;
    error <extensive>;
    init <extensive>;
    nat <extensive>;
    rm <extensive>;
  }
}
```

Hierarchy Level [edit security alg sccp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure Skinny Client Control Protocol (SCCP) tracing options.

Options *flag* —Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **call**—Enable tracing for SCCP call processing
- **cc**—Enable tracing for SCCP chassis cluster functions
- **cli**—Enable tracing for SCCP command-line interface (CLI) client processing
- **decode**—Enable tracing for SCCP decoder operations
- **error**—Enable tracing for SCCP processing errors
- **init**—Enable tracing for SCCP initialization errors
- **nat**—Enable tracing for SCCP NAT processing
- **rm**—Enable tracing for SCCP Resource Management (Resmgr) functions

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

traceoptions (Screen)

Syntax

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure screen tracing options.

To specify more than one tracing option, include multiple **flag** statements.

Options

filename —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number*** —(Optional) Specify the maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*** **.0,** then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*** **.0**. When the **trace-file** again reaches its maximum size, ***trace-file*** **.0** is renamed ***trace-file*** **.1** and ***trace-file*** is renamed ***trace-file*** **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

Copyright © 2011, Juniper Networks, Inc.

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all screen events
- **configuration**—Trace screen configuration events
- **flow**—Trace flow events

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

traceoptions (SCTP)

Syntax

```
traceoptions {
   file;
   flag {
      all;
      chassis-cluster;
      configuration;
      flow;
      parser;
   }
}
```

Hierarchy Level [edit security gprs sctp]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Set the trace options for Stream Control Transmission Protocol (SCTP).

Options

file—Name of the file in which to write the trace information.

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- **all**—Trace everything.
- **chassis-cluster**—Trace chassis cluster events.
- **configuration**—Trace configuration events.
- **flow**—Trace flow events.
- **parser**—Trace parser events.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (Security)

Syntax

```
traceoptions {
  file filename {
    <files number> ;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag flag ;
  no-remote-trace;
  rate-limit rate ;
}
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 8.5 of Junos OS.

Description Configure security tracing options.

Options

filename —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number*** —(Optional) Specify the maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*** **.0**, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*** **.0**. When the **trace-file** again reaches its maximum size, ***trace-file*** **.0** is renamed ***trace-file*** **.1** and ***trace-file*** is renamed ***trace-file*** **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events
- **configuration**—Trace security configuration events
- **compilation**—Trace security compilation events
- **routing-socket**—Trace routing socket events

no-remote-trace—Set remote tracing as disabled.

rate-limit *rate* —Number of trace per second. You can configure the incoming rate of trace messages.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (SIP ALG)

Syntax

```
traceoptions {
  flag {
    all <detail | extensive | terse>;
    call <detail | extensive | terse>;
    cc <detail | extensive | terse>;
    nat <detail | extensive | terse>;
    parser <detail | extensive | terse>;
    rm <detail | extensive | terse>;
  }
}
```

Hierarchy Level

[edit security alg sip]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure Session Initiation Protocol (SIP) tracing options.

Options

flag —Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace with all flags enabled
- **call**—Enable tracing for SIP call processing
- **cc**—Enable tracing for SIP chassis cluster functions
- **nat**—Enable tracing SIP Network Address Translation (NAT) processing
- **parser**—Enable tracing SIP parser operations
- **rm**—Enable tracing SIP Resource Management (Resmgr) functions

detail—Display moderate amount of data in trace.

extensive—Display extensive amount of data in trace.

terse—Display minimum amount of data in trace.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

traffic-options

Syntax

```
traffic-options {
sessions-per-client {
  limit value;
    over-limit (log-and-permit | block);
  }
}
```

Hierarchy Level [edit security utm utm-policy *policy-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

transaction-timeout

Syntax transaction-timeout *seconds* ;

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Timeout value for Media Gateway Control Protocol (MGCP) transactions. If the timeout value exceeds transaction will be removed by MGCP transactions ager out processing.

Options *seconds* —Timeout value.

Range: 3 through 50 seconds

Default: 30 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

trickling

Syntax

```
trickling {
   timeout value;
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus juniper-express-engine *profile-name*]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name*]
[edit security utm feature-profile anti-virus sophos-engine *profile-name*]

Release Information

Statement introduced in Release 9.5 of Junos OS. Statement updated in release 11.1 for Sophos support.

Description

HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. HTTP Trickling is time-based and there is only one parameter to configure for this feature, which is the timeout Interval. By default, trickling is disabled.

WARNING: When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.

Options

value —Timeout

Range: 0 through 600 seconds

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

trusted-ca

Syntax trusted-ca (*ca-index* | use-all);

Hierarchy Level [edit security group-vpn member ike policy *policy-name* certificate]
[edit security group-vpn server ike policy *policy-name* certificate]
[edit security ike policy *policy-name* certificate]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

Description Specify the preferred certificate authority (CA) to use when requesting a certificate from the peer. If no value is specified, then no certificate request is sent (although incoming certificates are still accepted). (This statement is not supported on dynamic VPN implementations.)

Options

- *ca-index* —Preferred certificate authority ID for the device to use.
- use-all—Device uses all configured certificate authorities.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

ttl

Syntax

```
ttl {
  match (equal | greater-than | less-than | not-equal);
  value time-to-live;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol ip]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value*time-to-live*—The time-to-live value.

Range: 0 through 255

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tunable-name

Syntax

```
tunable-name tunable-name {
  tunable-value protocol-value ;
}
```

Hierarchy Level [edit security idp sensor-configuration detector protocol-name *protocol-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the name of the tunable parameter to enable or disable the protocol detector for each of the service. By default, the protocol decoders for all services are enabled.

Options *tunable-name* —Name of the specific tunable parameter.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tunable-value

Syntax tunable-value *protocol-value* ;

Hierarchy Level [edit security idp sensor-configuration detector protocol-name *protocol-name* tunable-name *tunable-name*]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the value of the tunable parameter to enable or disable the protocol detector for each of the service.

Options *protocol-value* —Protocol number.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

tunnel

Syntax
```
tunnel {
  ipsec-group-vpn group-vpn;
  ipsec-vpn vpn-name ;
  pair-policy pair-policy ;
}
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information Statement introduced in Release 8.5 of Junos OS. **ipsec-group-vpn** option added in Release 10.2.

Description Encapsulate outgoing IP packets and decapsulate incoming IP packets.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

type (ICMP Headers in Signature Attack)

Syntax

```
type {
   match (equal | greater-than | less-than | not-equal);
   value type-value;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the primary code that identifies the function of the request/reply.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value*type-value*—Match a decimal value.

Range: 0 through 255

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

type (Dynamic Attack Group)

Syntax

```
type {
   values [anomaly | signature];
}
```

Hierarchy Level [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify an attack type filter to add attack objects based on the type of attack object (signature or protocol anomaly).

Options **values**—Name of the attack type filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

type (antivirus fallback-block)

Syntax type (message | protocol-only);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description You can configure notifications for both fallback blocking and fallback nonblocking actions. With protocol-only notifications, a protocol-specific error code may be returned to the client.

Options
- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

type (antivirus feature-profile)

Syntax type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS. Statement updated for Sophos in Release 11.1 of Junos OS.

Description Set the antivirus engine that will be used on the device. You can only have one engine type running and you must restart the device if you change engines.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

type (antivirus notification-options virus-detection)

Syntax type (message | protocol-only);

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options virus-detection]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description When content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code may be returned to the client.

Options
- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

type (content-filtering notification-options)

Syntax type (message | protocol-only);

Hierarchy Level [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description When content is blocked, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code may be returned to the client.

Options
- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

udp (Protocol Binding Custom Attack)

Syntax

```
udp {
   minimum-port port-number maximum-port port-number;
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Allow IDP to match the attack for specified UDP port(s).

Options

minimum-port*port-number*—Minimum port in the port range.

Range: 0 through 65,535

maximum-port*port-number*—Maximum port in the port range.

Range: 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

udp (Security Screen)

Syntax

```
udp {
  flood {
    threshold number ;
  }
  udp-sweep {
    threshold threshold number;
  }
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the number of packets allowed per second to the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

udp (Signature Attack)

Syntax

```
udp {
  data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length ;
  }
  destination-port {
    match (equal | greater-than | less-than | not-equal);
    value destination-port ;
  }
  source-port {
    match (equal | greater-than | less-than | not-equal);
    value source-port ;
  }
}
```

Hierarchy Level

[edit security idp custom-attack *attack-name* attack-type signature protocol]

Release Information

Statement introduced in Release 9.3 of Junos OS.

Description

Allow IDP to match the UDP header information for the signature attack.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

udp-sweep

Syntax

```
udp-sweep {
   threshold number;
}
```

Hierarchy Level

[edit security screen ids-option *screen-name* udp]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Configure the device to detect and prevent UDP sweep attack. In a UDP sweep attack, an attacker sends UDP packets to the target device. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further UDP packets from that host for the remainder of the specified threshold period.

Options

threshold *number*—Maximum number of microseconds during which up to 10 UDP packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers an UDP Sweep attack response on the device during the remainder of the second.

Range: 1000 through 1,000,000 microseconds

Default: 5000 microseconds

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

unknown-message (H.323 ALG)

Syntax

```
unknown-message {
   permit-nat-applied;
   permit-routed;
}
```

Hierarchy Level [edit security alg h323 application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify how unidentified H.323 messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options

permit-nat-applied—Specify that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

unknown-message (MGCP ALG)

Syntax

```
unknown-message {
   permit-nat-applied;
   permit-routed;
}
```

Hierarchy Level [edit security alg mgcp application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify how unidentified Media Gateway Control Protocol (MGCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options

permit-nat-applied—Specify that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

unknown-message (SCCP ALG)

Syntax

```
unknown-message {
   permit-nat-applied;
   permit-routed;
}
```

Hierarchy Level [edit security alg sccp application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify how unidentified Skinny Client Control Protocol (SCCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options

permit-nat-applied—Specify that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

unknown-message (SIP ALG)

Syntax

```
unknown-message {
   permit-nat-applied;
   permit-routed;
}
```

Hierarchy Level [edit security alg sip application-screen]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify how unidentified Session Initiation Protocol (SIP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SIP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options

permit-nat-applied—Specify that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

upload-profile (ftp antivirus utm-profile)

Syntax upload-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus ftp]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

upload-profile (ftp content-filtering utm-profile)

Syntax upload-profile *profile-name*;

Hierarchy Level [edit security utm utm-policy *policy-name* content-filtering ftp]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

urgent-pointer

Syntax

```
urgent-pointer {
   match (equal | greater-than | less-than | not-equal);
   value urgent-pointer;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the data in the packet is urgent; the URG flag must be set to activate this field.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***urgent-pointer*** —Match the value of the urgent pointer.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

uri-check

Syntax uri-check;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine *profile-name* scan-options]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is a way of analyzing URI content in HTTP traffic against a remote Sophos database to identify malware or malicious content. URI checking is on by default.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

url

Syntax url *url-name* ;

Hierarchy Level [edit security idp security-package]

Release Information Statement introduced in Release 9.2 of Junos OS.

Description Specify the URL to automatically download the updated signature database.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

url (kaspersky-lab-engine)

Syntax *url*;

Hierarchy Level [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description This is the command for changing the URL for the pattern database. The default URL is http://update.juniper-update.net/AV/SRX210. You should not change this URL unless you are experiencing problems with it and have called for support.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

url (juniper-express-engine)

Syntax *url*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine pattern-update]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description This is the command for changing the URL for the pattern database. You should not change this URL unless you are experiencing problems with it and have called for support.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

url (Sophos pattern-update)

Syntax url *url*;

Hierarchy Level [edit security utm feature-profile anti-virus sophos-engine pattern-update]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Change the default URL used to retrieve the Sophos pattern data files. You should not change this URL unless you are experiencing problems with it and have called for support.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

url-blacklist

Syntax
```
url-blacklist {
listname;
}
```

Hierarchy Level [edit security utm feature-profile web-filtering]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description This is a global blacklist category, blocking content for web-filtering.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

url-pattern

Syntax

```
url-pattern {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use URL Pattern Lists to create Custom URL Category Lists. These are lists of patterns that bypass scanning.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

url-whitelist (antivirus)

Syntax

```
url-whitelist {
listname;
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description A URL white list is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

url-whitelist (web-filtering)

Syntax

```
url-whitelist {
listname;
}
```

Hierarchy Level [edit security utm feature-profile web-filtering]

Description A URL white list is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

user

Syntax

```
user {
  username;
}
```

Hierarchy Level [edit security dynamic-vpn client *configuration-name*]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Use this statement to specify which users can access the selected dynamic VPN configuration.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

user-at-hostname

Syntax **user-at-hostname** ***user-at-hostname*** **;**

Hierarchy Level [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description Configure an e-mail address. (This statement is not supported on dynamic VPN implementations.)

Options ***user-at-hostname*** —Valid e-mail address.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

utm

Syntax

```
utm {
custom-objects {
  filename-extension {
    value [list];
    }
    mime-pattern {
    value [list];
    }
    custom-url-category {
    value [list];
    }
    protocol-command {
    value [list];
    }
    url-pattern {
    value [list];
    }
  }
  feature-profile {
  anti-virus {
    type kaspersky-lab-engine;
      kaspersky-lab-engine {
      pattern-update {
        url;
          interval value;
        }
        profile profile-name {
        fallback-options {
          default (log-and-permit | block);
            corrupt-file (log-and-permit | block);
            password-file (log-and-permit | block);
            decompress-layer (log-and-permit | block);
            content-size (log-and-permit | block);
            engine-not-ready (log-and-permit | block);
            timeout (log-and-permit | block);
            out-of-resources (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
          scan-options {
          intelligent-prescreening;
            scan-mode (scan-all | by--extension);
            content-size-limit value;
            timeout value;
            decompress-layer-limit value;
          }
          notification-options {
          virus-detection {
            type (message | protocol-only);
              notify-mail-sender;
              custom-message;
            }
            fallback-block {
```

```
            custom-message;
              notify-mail-sender;
              type;
            }
          }
          trickling {
            timeout value;
          }
        }
      }
      type juniper-express-engine;
      juniper-express-engine {
      pattern-update {
        url;
          interval value;
        }
        profile profile-name {
        fallback-options {
          default (log-and-permit | block);
            content-size (log-and-permit | block);
            engine-not-ready (log-and-permit | block);
            timeout (log-and-permit | block);
            out-of-resources (log-and-permit | block);
            too-many-requests (log-and-permit | block);
          }
          scan-options {
          intelligent-prescreening;
            scan-mode (scan-all | by--extension);
            content-size-limit value;
            timeout value;
            decompress-layer-limit value;
          }
          notification-options {
          virus-detection {
            type (message | protocol-only);
              notify-mail-sender;
              custom-message;
            }
            fallback-block {
            custom-message;
              notify-mail-sender;
              type;
            }
          }
          trickling {
            timeout value;
          }
        }
        mime-whitelist {
        list listname {
          exception listname;
        }
        url-whitelist {
        listname;
        }
      }
```


Copyright © 2011, Juniper Networks, Inc.

```
}
web-filtering {
surf-control-integrated {
  cache {
    timeout value;
    }
    server {
    host host-name;
      port number;
    }
  profile profile-name{
    default (log-and-permit | block);
      custom-block-message value;
      fallback-settings {
      default (log-and-permit | block);
        server-connectivity (log-and-permit | block);
        timeout (log-and-permit | block);
        too-many-requests (log-and-permit | block);
      }
      category customurl-list name {
      action (log-and-permit | block);
      }
    }
  websense-redirect {
  profile profile-name {
  server {
    host host-name;
      port number;
    }
    sockets value;
      timeout value;
      fallback-settings {
      default (log-and-permit | block);
        server-connectivity (log-and-permit | block);
        timeout (log-and-permit | block);
        too-many-requests (log-and-permit | block);
      }
    }
  url-whitelist {
  listname;
  }
  url-blacklist {
  listname;
  }
}
anti-spam {
sbl {
  profile profile-name{
    sbl-default-server;
      spam-action (log-and-permit | block);
      custom-tag-string [***SPAM***];
    }
    address-whitelist{
    listname;
    }
  }
```

```
        }
        content-filtering {
        profile profile-name{
          block-command protocol-command-list;
            block-content-type (java-applet | exe | http-cookie);
            block-mime {
            list list-name {
              exception list-name;
              }
            }
          permit-command protocol-command-list;
          notification-options {
          type (message | protocol-only);
            custom-message [message];
          }
        }
      }
      utm-policy policy-name {
      anti-virus {
        http-profile profile-name;
          ftp {
          upload-profile profile-name;
            download-profile profile-name;
          }
          smtp-profile profile-name;
          pop3-profile profile-name;
          imap-profile profile-name;
        }
        content-filtering {
        http-profile profile-name;
          ftp {
          upload-profile profile-name;
            download-profile profile-name;
          }
          smtp-profile profile-name;
          pop3-profile profile-name;
          imap-profile profile-name;
        }
        anti-spam {
        smtp-profile profile-name;
        }
        web-filtering {
        http-profile profile-name;
        }
        traffic-options {
        sessions-per-client {
          limit value;
            over-limit (log-and-permit | block);
          }
        }
      }
    }
```

Hierarchy Level [edit security]

Copyright © 2011, Juniper Networks, Inc.

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure UTM features.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

utm-policy

Syntax

```
utm-policy policy-name {
anti-virus {
  http-profile profile-name;
    ftp {
    upload-profile profile-name;
      download-profile profile-name;
    }
    smtp-profile profile-name;
    pop3-profile profile-name;
    imap-profile profile-name;
  }
  content-filtering {
  http-profile profile-name;
    ftp {
    upload-profile profile-name;
      download-profile profile-name;
    }
    smtp-profile profile-name;
    pop3-profile profile-name;
    imap-profile profile-name;
  }
  anti-spam {
  smtp-profile profile-name;
  }
  web-filtering {
  http-profile profile-name;
  }
  traffic-options {
  sessions-per-client {
    limit value;
      over-limit (log-and-permit | block);
    }
  }
}
```

Hierarchy Level [edit security utm]

Release Information Statement introduced in Release 9.5 of Junos OS.

Description Configure a UTM policy for antivirus, antispam, content-filtering, and web-filtering protocols and attach this policy to a security profile to implement it.

Options The remaining statements are explained separately.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

value-hit-rate-threshold

Syntax

```
context <context-name> {
   value-hit-rate-threshold number;
}
```

Hierarchy Level

[edit security idp application-ddos *name* context *context-name*]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure the context-value-hit-rate threshold in tick interval. A tick is defined as 60 seconds by default. When the same context value is requested for more than value-hit-rate-threshold limit for a given context and application-level distributed denial-of-service (DDoS) application, the system will start bot client classification, if time-binding parameters are configured. If time-binding parameters are not configured, the configured policy actions are taken.

NOTE: If time-binding is not configured, the system will skip bot client classification, and the configured policy actions are taken. This could result in valid clients being applied with configured policy actions. Time-binding configuration (count and period) should be used for bot client classification. However, this feature can be used as an Application Layer screen to deny resource access for all clients when context value-hit-rate-threshold is exceeded.

Options

number —Context value hit rate threshold.

Range:

- SRX3400– 1 to 250,000,000
- SRX3600–1 to 500,000,000
- SRX5600/5800–1 to 2,500,000,000

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

virus-detection

Syntax

```
virus-detection {
type (message | protocol-only);
  notify-mail-sender;
  custom-message;
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus juniper-express-engine *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* notification-options]

Release Information

Statement introduced in Release 9.5 of Junos OS.

Description

Configure a notification to send when a virus is detected.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

virus-detection (Sophos antivirus notification-options)

Syntax

```
virus-detection {
  custom-message message;
  custom-message-subject subject;
  no-notify-mail-sender;
  notify-mail-sender;
  type (protocol-only | message );
}
```

Hierarchy Level

[edit security utm feature-profile anti-virus sophos-engine *profile-name* notification-options]

Release Information

Statement introduced in Release 11.1 of Junos OS.

Description

Configure notification options that will occur when a virus is detected.

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

vpn

Syntax

```
vpn vpn-name ;
bind-interface interface-name ;
df-bit (clear | copy | set);
establish-tunnels (immediately | on-traffic);
ike {
  gateway gateway -name ;
  idle-time seconds ;
  install-interval seconds ;
  ipsec-policy ipsec-policy-name ;
  no-anti-replay;
  proxy-identity {
    local ip-prefix ;
    remote ip-prefix ;
    service service-name ;
  }
}
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key );
  }
  encryption {
    algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    key (ascii-text key | hexadecimal key );
  }
  external-interface external-interface-name ;
  gateway ip-address ;
  protocol (ah | esp);
  spi spi-value ;
}
vpn-monitor {
  destination-ip ip-address ;
  optimized;
  source-interface interface-name ;
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

Description Configure an IPsec VPN.

Options *vpn-name* —Name of the VPN.

The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

vpn-monitor

Syntax

```
vpn-monitor {
   destination-ip ip-address ;
   optimized;
   source-interface interface-name ;
}
```

Hierarchy Level

[edit security ipsec vpn *vpn-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Configure settings for VPN monitoring. This feature cannot be configured simultaneously with the **dead-peer-detection** statement. (This statement is not supported on dynamic VPN implementations.)

Options

The remaining statements are explained separately.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- **dead-peer-detection on page 395**
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

vpn-monitor-options

Syntax

```
vpn-monitor-options {
   interval seconds ;
   threshold number ;
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure VPN monitoring options. (This statement is not supported on dynamic VPN implementations.)

Options

interval ***seconds*** —Interval at which to send ICMP requests to the peer.

Range: 1 through 3600 seconds

Default: 10 seconds

threshold ***number*** —number of consecutive unsuccessful pings before the peer is declared unreachable.

Range: 1 through 65536 pings

Default: 10 pings

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

web-authentication

Syntax

```
web-authentication {
  client-match user-or-group ;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that the policy allows access to users who have previously been authenticated by Web authentication. Web authentication must be enabled on one of the addresses on the interface to which the HTTP request is redirected.

Options

client-match ***user-or-group*** —(Optional) Username or user group name.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

web-redirect

Syntax web-redirect;

Hierarchy Level [edit security policies from-zone *zone-name* to zone *zone-name*policy *policy-name* then permit firewall-authentication pass-through]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Optionally, redirect HTTP requests to the device's internal webserver by sending a redirect HTTP response to the client system to reconnect to the webserver for user authentication. The interface on which the client's request arrived is the interface to which the request is redirected.

Using this feature allows for a richer user login experience. For example. instead of a popup prompt asking for username and password, users can get the login page in a browser. Enabling **web-redirect** has the same effect as users typing the Web authentication IP address in a client browser. Using **web-redirect** provides a more seamless authentication experience because users do not need to know the Web authentication IP address but only the IP address of the resource they are trying to access. After the user has been authenticated this way, traffic from user's IP address is authenticated to go through the **web-redirect** method.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

weight

Syntax

```
weight {
   equal;
   firewall;
   idp;
}
```

Hierarchy Level [edit security forwarding-process application-services maximize-idp-sessions]]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity.

Devices ship with an implicit default session capacity setting. This default value gives more weight to firewall sessions. You can manually override the default by using the **maximize-idp-sessions** command. The command allows you to choose between these weight values: **equal**, **firewall**, and **IDP**. The following table displays the available session capacity weight and approximate throughput for each.

Table 5: Session Capacity and Resulting Throughput

Weight Value	Firewall Capacity	IDP Capacity	Firewall Throughput	IDP Throughput
Default	1,000,000	256,000	10 Gbps	2.4 Gbps
Equal	1,000,000	1,000,000	8.5 Gbps	2 Gbps
Firewall	1,000,000	1,000,000	10 Gbps	2.4 Gbps
IDP	1,000,000	1,000,000	5.5 Gbps	1.4 Gbps

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

wildcard

Syntax wildcard *string*;

Hierarchy Level [edit security group-vpn server ike gateway *gateway-name* dynamic distinguished-name]
[edit security ike gateway *gateway-name* dynamic distinguished-name]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

Description Specify that the values of a dynamic virtual private network (VPN) endpoint user's distinguished name's identity fields match the values in the group IKE user's distinguished name's fields. The order of the identity fields in the distinguished name strings does not matter during a match. (This statement is not supported on dynamic VPN implementations.)

Options ***string***—Distinguished name identity values to be matched.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

window-scale

Syntax
```
window-scale {
   match (equal | greater-than | less-than | not-equal);
   value window-scale-factor;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the scale factor that the session of the attack will use. The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value ***window-scale-factor***—Match the number of bytes.

Range: 0 through 255

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

window-size

Syntax

```
window-size {
   match (equal | greater-than | less-than | not-equal);
   value window-size;
}
```

Hierarchy Level [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

Release Information Statement introduced in Release 9.3 of Junos OS.

Description Specify the number of bytes in the TCP window size.

Options **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

value*window-size*—Match the number of bytes.

Range: 0 through 65,535

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

winnuke

Syntax winnuke;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable detection of attacks on Windows NetBios communications. Packets are modified as necessary and passed on. Each WinNuke attack triggers an attack log entry in the event alarm log.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

xauth

Syntax

```
xauth {
  access-profile profile-name ;
}
```

Hierarchy Level

[edit security ike gateway *gateway-name*]

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify that extended authentication (XAuth) is performed in addition to IKE authentication for remote users trying to access a VPN tunnel. Include a previously created access profile, created with the **edit access profile** statement, to specify the access profile to be used for authentication information.

Options

access-profile *profile-name* —Name of previously created access profile to reference for authentication information.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS System Basics Configuration Guide*
- *Junos OS Security Configuration Guide*

zones

Syntax

```
zones {
  functional-zone {
    management {
      host-inbound-traffic {
        protocols {
          protocol-name ;
          protocol-name <except>;
        }
        system-services {
          service-name ;
          service-name <except>;
        }
      }
      interfaces interface-name {
        host-inbound-traffic {
          protocols {
            protocol-name ;
            protocol-name <except>;
          }
          system-services {
            service-name ;
            service-name <except>;
          }
        }
      }
      screen screen-name ;
    }
  }
  security-zone zone-name {
    address-book {
      address address-name ( ip-prefix | dns-name dns-address-name | wildcard-address
        ipv4–address/wildcard-mask ) ;
      address-set address-set-name {
        address address-name ;
      }
    }
    host-inbound-traffic {
      protocols {
        protocol-name ;
        protocol-name <except>;
      }
      system-services {
        service-name ;
        service-name <except>;
      }
    }
    interfaces interface-name {
      host-inbound-traffic {
        protocols {
          protocol-name ;
          protocol-name <except>;
        }
```


Copyright © 2011, Juniper Networks, Inc.

```
            system-services {
              service-name ;
              service-name  <except>;
            }
          }
        }
        screen  screen-name ;
        tcp-rst;
      }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 19

Services Hierarchy and Statements

This section contains the following topics:

- Services Configuration Statement Hierarchy on page 857

Services Configuration Statement Hierarchy

Use the statements in the **services** configuration hierarchy to configure application identification, RPM probes, and Unified Access Control.

```
services {
  application-identification {
    application application-name {
      disable;
      index;
      signature {
        client-to-server {
          dfa-pattern pattern;
          regex;
        }
        disable;
        min-data bytes;
        order;
        port-range {
          tcp <TCP-port-range>;
          udp <UDP-port-range>;
        }
        server-to-client {
          dfa-pattern pattern;
          regex;
        }
      }
      type name;
    }
    application-system-cache-timeout value;
    download {
      automatic {
        interval hours;
        start-time  MM-DD.hh:mm;
      }
      url url;
    }
```

```
    enable-heuristics;
    max-checked-bytes bytes;
    max-sessions value;
    nested-application name {
      index;
      protocol;
      signature name {
        chain-order;
        maximum-transactions;
        member name {
          context [http-header-content-type | http-header-host | http-url-parsed |
            http-url-parsed-param-parsed];
          direction [any | client-to-server | server-to-client];
          pattern dfa-pattern;
        }
        order value;
      }
      type name;
    }
    nested-application-settings {
      no-application-system-cache;
      no-nested-application;
    }
    no-application-identification;
    no-application-system-cache;
    traceoptions {
      file filename <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>
      flag all;
      no-remote-trace;
    }
  }
  unified-access-control {
    captive-portal policy {
      redirect-traffic (all | unauthenticated);
      redirect-url url;
    }
    infranet-contoller hostname {
      address ip-address;
      port port-number;
      interface interface-name;
      password password;
      ca-profile ca-profile;
      server-certificate-subject subject;
    }
    timeout seconds;
    interval seconds;
    timeout-action (close | no-change | open):
  test-only-mode (true | false):
    traceoptions {
      flag [ (ipc | config | connect | all) ];
    }
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Services Interfaces Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

address

Syntax address *ip-address*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the IP-address of the Infranet Controller with which the SRX Series devices should communicate.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **infranet-controller on page 871**
- *Junos OS Security Configuration Guide*

application

Syntax

```
application application-name {
  disable;
  index;
  signature {
    client-to-server {
      dfa-pattern pattern;
      regex;
    }
    disable;
    min-data bytes;
    order;
    port-range{
      tcp <TCP-port-range>;
      udp <UDP-port-range>;
    }
    server-to-client {
      dfa-pattern pattern;
      regex;
    }
  }
  type name;
}
```

Hierarchy Level

[edit services application-identification]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Configure a custom application definition for the desired application name that will be used by the system to identify the application as it passes through the device. Custom application definitions can be used for applications that are not part of the Juniper Networks predefined application database.

Options

disable—Do not match traffic for this application. Default is off.

index—A number that is a one-to-one mapping to the application name that is used to ensure that each signature definition is unique. The index range for predefined applications is 1 through 32767. The index range for custom applications and custom nested applications is 32768 through 65534. (Required)

type *name*—Well known application name name, such as FTP, TELNET, HTTP. Must be a unique name with a maximum length of 32 characters. (Required)

The remaining statements are explained separately.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

application–identification

Syntax

```
application-identification {
  application application-name {
    disable;
    index;
    signature {
      client-to-server {
        dfa-pattern pattern;
        regex;
      }
      disable;
      min-data bytes;
      order;
      port-range {
        tcp <TCP-port-range>;
        udp <UDP-port-range>;
      }
      server-to-client {
        dfa-pattern pattern;
        regex;
      }
    }
    type name;
  }
  application-system-cache-timeout value;
  download {
    automatic {
      interval hours;
      start-time  MM-DD.hh:mm;
    }
    url url;
  }
  enable-heuristics;
  max-checked-bytes bytes;
  max-sessions value;
  nested-application name {
    index;
    protocol;
    signature name {
      chain-order;
      maximum-transactions;
      member name {
        context [http-header-content-type | http-header-host | http-url-parsed |
          http-url-parsed-param-parsed];
        direction [any | client-to-server | server-to-client];
        pattern dfa-pattern;
      }
      order value;
    }
    type name;
  }
  nested-application-settings {
    no-application-system-cache;
```

```
    no-nested-application;
  }
  no-application-identification;
  no-application-system-cache;
  traceoptions {
    file filename <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>
    flag all;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit services]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure application identification options to identify the TCP/UDP application session running on nonstandard ports to match the application properties of transiting network traffic.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

ca-profile

Syntax ca-profile *ca-profile*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the certificate authority (CA) of the certificate that the SRX Series device should use in communications with an Infranet Enforcer. The SRX Series device uses the CA to validate the Infranet Controller's server certificate.

Use this statement if you have loaded certificates from multiple certificate authorities (CAs) onto your SRX Series device and you need to configure the device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- **server-certificate-subject on page 881**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

captive-portal

Syntax

```
captive-portal policy {
   redirect-traffic (all | unauthenticated);
   redirect-url url;
}
```

Hierarchy Level

[edit services unified-access-control]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Specify the preconfigured security policy for captive portal on the Junos OS Enforcer to enable the captive portal feature. The captive portal policy is configured as part of the UAC policy.

By configuring the captive portal feature, you can redirect traffic destined for protected resources to the Infranet Controller or to the URL you configure on the Junos OS Enforcer.

Options

The remaining statements are explained separately.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **captive-portal (Unified Access Control policy) on page 864**
- **redirect-traffic on page 879**
- **redirect-url on page 880**
- *Junos OS Security Configuration Guide*

captive-portal (Unified Access Control policy)

Syntax captive-portal *captive-portal-policy-name*;

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services uac-policy]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Create the captive portal policy in the UAC security policy. You use the captive portal policy to configure the captive portal feature on the Junos OS Enforcer. By configuring the captive portal feature, you can redirect traffic destined for protected resources to the Infranet Controller or to the URL you configure on the Junos OS Enforcer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- **captive-portal on page 863**
- **redirect-traffic on page 879**
- **redirect-url on page 880**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

download

Syntax

```
download {
  automatic {
    interval hours;
    start-time MM-DD.hh:mm;
  }
url url;
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure automatic download for the application identification services application package. The application package contains definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP. The application package is extracted from the IDP signature database located at https://services.netscreen.com/cgi-bin/index.cgi. If you do not have access to the default download site from your device, you can use the URL option to download from a different location.

NOTE: You need to download the application package before configuring application identification services.

Options

automatic —Download the application package automatically at a certain time of day or at intervals.

interval —Download the application package at intervals.

Range: 6 through 720 hours

start-time —Start time in which the application package will be download. Format is MM-DD.hh:mm. Example: 04-15.09:00 will start the download on April 15 at 9 AM.

url —Use this option to change the default download location of the application package.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

dscp-rewrite

Syntax

```
dscp-rewrite {
   code-point 6 bit patterns;
}
```

Hierarchy Level

[edit security alg sip]
[edit security alg h323]
[edit security alg mgcp]
[edit security alg sccp]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Specify a rewrite-rule for the traffic that passes through a voice over IP Application Layer Gateway (VoIP ALG).

Options

6-bit patterns—Value of the code point in binary form.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

enable-heuristics

Syntax

enable-heuristics;

Hierarchy Level

[edit services application-identification]

Release Information

Statement introduced in Release 11.1 of Junos OS.

Description

The **enable-heuristics** command is an optional command and is off by default. It enables encryption and P2P detection.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

flow-monitoring

Syntax flow-monitoring

Hierarchy Level [edit services]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure flow monitoring.

Options
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **version9**—Version 9 configuration.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

flow-monitoring version 9

Syntax version9

Hierarchy Level [edit services flow-monitoring]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Version 9 configuration.

Options
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **template**—One or more version 9 templates.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

flow-monitoring version 9 template

Syntax template *name*

Hierarchy Level [edit services flow-monitoring version9]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description One or more version 9 templates.

Options

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **flow-active-timeout (10...600)**—Interval after which active flow is exported.
- **flow-inactive-timeout (10...600)**—Period of inactivity that marks a flow inactive.
- **ipv4-template**—IPv4 template configuration.
- **option-refresh-rate**—Option template refresh rate.
- **template-refresh-rate**—Template refresh rate.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

flow-server

Syntax flow-server *address*

Hierarchy Level [edit forwarding-options sampling family inet output flow-server]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure sending traffic aggregates in cflowd format.

Options

- **aggregation (version 8 only)**—Aggregations to perform for exported flows.
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **autonomous-system-type**—Type of autonomous system number to export.
- **local-dump**—Dump cflowd records to log file before exporting.
- **no-local-dump**—Donot dump cflowd records to log file before exporting.
- **port**—UDP port number on host collecting cflowd packets.
- **source-address**—Source IPv4 address for cflowd packets.
- **version**—Format of exported cflowd aggregates..
- **version9**—Exported data in version 9 format.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

flow-server version 9

Syntax version9

Hierarchy Level [edit forwarding-options sampling family inet output flow-server]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Export data in version 9 format.

Options

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **template**—Template configuration.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

infranet-controller

Syntax

```
infranet-contoller hostname {
   address ip-address;
   port port-number;
   interface interface-name;
   password password;
   ca-profile ca-profile;
   server-certificate-subject subject;
}
```

Hierarchy Level

[edit services unified-access-control]

Release Information

Statement introduced in Release 9.4 of Junos OS.

Description

Specify the hostname of the Infranet Controller with which the SRX Series devices should communicate. Possible values for this statement range from 1 to 31 characters.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options

The remaining statements are explained separately.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **address on page 859**
- *Junos OS Security Configuration Guide*

inline-jflow

Syntax inline-jflow

Hierarchy Level [edit forwarding-options sampling family inet output]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Inline processing of sampled packets.

Options

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **source-address**—Address to use for generating monitored packets.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

interface

Syntax interface *interface-name*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the SRX Series interface through which the Infranet Controller should connect.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **port on page 878**
- **password on page 877**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

interval

Syntax interval *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the value in seconds that the SRX Series device should expect to receive a heartbeat signal from the Infranet Controller (default 30). This configuration statement is used in conjunction with the **timeout** statement to test active communications with the Infranet Controller. The value of the **interval** statement must be smaller than the value of **timeout** statement.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **timeout on page 885**
- **timeout-action on page 886**
- *Junos OS Security Configuration Guide*

max-checked-bytes

Syntax max-checked-bytes *bytes*;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description The maximum number of bytes to be applied with the application signatures.

Options *bytes* —Maximum bytes.
Range: 0 through 100000 bytes
Default: 100000 bytes

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

nested-application

Syntax

```
nested-application name {
  index;
  protocol;
  signature name {
    chain-order;
    maximum-transactions;
    member name {
      context [http-header-content-type | http-header-host | http-url-parsed |
        http-url-parsed-param-parsed];
      direction [any | client-to-server | server-to-client];
      pattern dfa-pattern;
    }
    order value;
  }
  type name;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device. Custom nested application definitions can be used for nested applications that are not part of the Juniper Networks predefined nested application database.

Options

index—A number that is a one-to-one mapping to the application name that is used to ensure that each signature definition is unique. The index range for predefined applications is 1 through 32767. The index range for custom applications and custom nested applications is 32768 through 65534. (Required)

protocol—The protocol that will be monitored to identify nested applications. HTTP is supported.

signature *name*—Name of the custom nested application signature definition. Must be a unique name with a maximum length of 32 characters. (Required)

chain-order—Signatures can contain multiple members. If chain-order is on, those members are read in order. The default for this option is no chain order. If a signature only contains one member, this option is ignored.

maximum-transactions—The maximum number of transactions that should occur before a match is made.

member *name*—Defines a member name for a custom nested application signature definition. Custom definitions can contain multiple members that define attributes for an application.

context—Define a service specific context, such as http-url.

Copyright © 2011, Juniper Networks, Inc.

direction—The connection direction of the packets to apply pattern matching. The options are client-to-server, server-to-client, or any.

pattern *dfa-pattern*—Define the DFA pattern to match in the context.

order—When there are multiple patterns matched for the same session, the lowest order number takes the highest priority. Must be unique. (Required)

type—Well known application name for this application definition, such as Facebook and Kazza. Must be a unique name with a maximum length of 32 characters. (Required)

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

nested-application-settings

Syntax

```
nested-application-settings {
  no-application-system-cache;
  no-nested-application;
}
```

Hierarchy Level
[edit services application-identification]

Release Information
Statement introduced in Release 10.2 of Junos OS.

Description
Configure nested application options for application identification services.

Options

no-application-system-cache—Nested application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the no-application-system-cache statement to turn it off.

no-nested-application—Sometimes there is a need to identify multiple different applications running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols. This function is turned on by default. Use the no-nested-application statement to turn it off.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-application-identification

Syntax no-application-identification;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Disable the TCP/UDP application identification of applications running on nonstandard ports.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

no-application-system-cache

Syntax no-application-system-cache;

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-application-system-cache** statement to turn it off.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

option-refresh-rate

Syntax option-refresh-rate

Hierarchy Level [edit services flow-monitoring version9 template]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Option template refresh rate.

Options

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **packets**—In number of packets (1...480000).
- **seconds**—In number of seconds(10...600).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

password

Syntax password *password*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the password that the SRX Series device should send to the Infranet Controller in order to establish communications. The SRX Series device sends the password in its first message to the Infranet Controller.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **ca-profile on page 862**
- **server-certificate-subject on page 881**
- *Junos OS Security Configuration Guide*

port

Syntax port *port-number*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the port on the Infranet Controller through which the SRX Series device should establish connections (default 11123). Possible values for this statement range from 1 through 65,535.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **interface on page 872**
- **password on page 877**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

redirect-traffic

Syntax redirect-traffic (all | unauthenticated);

Hierarchy Level [edit services unified-access-control captive-portal *policy*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify to redirect traffic destined for protected sources to the Infranet Controller. You can choose to redirect all traffic or only unauthenticated traffic.

Options

all—Redirect all traffic destined for the protected sources to the Infranet Controller. Specify this option if you want to redirect all traffic (IPsec or source IP) to the currently connected Infranet Controller or to an IP address or domain name that you specify in a redirect URL

unauthenticated—Redirect unauthenticated traffic destined for the protected sources to the Infranet Controller. Select this option if your deployment uses source IP only or a combination of source IP and IPsec. The Junos OS Enforcer redirects clear-text traffic from unauthenticated users to the currently connected Infranet Controller or to an IP address or domain name that you specify in a redirect URL.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **captive-portal on page 863**
- **captive-portal (Unified Access Control policy) on page 864**
- **redirect-url on page 880**
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

redirect-url

Syntax redirect-url *url*;

Hierarchy Level [edit services unified-access-control captive-portal *policy*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Specify to redirect traffic destined for protected sources to a specified URL.

You can configure the following options in the redirect URL string:

- ***%dest-url%***—Specifies the protected resource which the user is trying to access.
- ***%enforcer-id%***—Specifies the ID assigned to the Junos OS Enforcer by the Infranet Controller.
- ***%policy-id%***—Specifies the encrypted policy ID for the security policy that redirected the traffic.
- ***%dest-ip%***—Specifies the IP address or hostname of the protected resource that the user is trying to access.
- ***%ic-ip%***—Specifies the IP address or hostname of the Infranet Controller to which the Junos OS Enforcer is currently connected to.

If you do not specify the redirect URL, the Junos OS Enforcer uses the following default configuration:

```
https://%ic-ip%/?target = %dest-url%  &enforcer = %enforcer-id%  &policy =
%policy-id%  &dest-ip = %dest-ip%
```

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **captive-portal on page 863**
- **captive-portal (Unified Access Control policy) on page 864**
- **redirect-traffic on page 879**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

server-certificate-subject

Syntax server-certificate-subject *subject*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Optionally specify the full subject name of the certificate that the SRX Series device should use to validate the Infranet Controller's server certificate.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **ca-profile on page 862**
- **password on page 877**
- *Junos OS Security Configuration Guide*

signature

Syntax

```
signature {
  client-to-server {
    dfa-pattern pattern;
    regex;
  }
  disable;
  min-data bytes;
  order;
  port-range {
    tcp <TCP-port-range>;
    udp <UDP-port-range>;
  }
  server-to-client {
    dfa-pattern pattern;
    regex;
  }
}
```

Hierarchy Level [edit services application-identification application *application-name*]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure the signature attributes for a custom application definition.

Options

client-to-server—Define the attributes for traffic in the client to server direction.

dfa-pattern—Define the dfa pattern for the application traffic in the client-to-server direction. Maximum length is 1023.

regex—Enter a regular expression that should be matched for client to server traffic.

disable—Toggle on means signature method is not used to identify this application. Default is off.

min-data—The minimum number of bytes or packets to apply to the dfa-pattern. Default is 10, range is 4 through 1024.

order—When there are multiple patterns matched for the same session, the lowest order number takes the highest priority. Must be unique. (Required)

port-range [*tcp* | *udp*]—Define the port range for the application. Default ranges: TCP/0 through 65,535, UDP/0 through 65,535. (Optional)

server-to-client—Define the attributes for traffic in the server to client direction.

dfa-pattern—Define the dfa pattern for the application traffic in the server to client direction. Maximum length is 1023.

regex—Enter a regular expression that should be matched for server to client traffic.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

template-refresh-rate

Syntax
template-refresh-rate

Hierarchy Level
[edit services flow-monitoring version9 template]

Release Information
Statement introduced in Release 10.4 of Junos OS.

Description
Template refresh rate.

Options
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **packets**—In number of packets (1...480000).
- **seconds**—In number of seconds (10...600).

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

test-only-mode

Syntax test-only-mode (true | false):

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Configure the device in test-only mode to log access decisions from the Infranet Controller without actually enforcing the decisions. When configured in test-only mode, the SRX Series device enables all UAC traffic to go through so you can test the implementation without impeding traffic.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

timeout

Syntax timeout *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify the value in seconds that the SRX Series device should wait to get a heartbeat response from an Infranet Controller (default 60). If the SRX Series device does not receive a response in the specified time, it takes the action specified by the **timeout-action** configuration statement. It also tries again to make a connection to the Infranet Controller. After the second failed attempt, the SRX Series device fails over to the next Infranet Controller in the cluster. The SRX Series device continues trying to reach Infranet Controllers in the cluster until a connection is established.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller. When working with a cluster of Infranet Controllers, the Junos OS Enforcer connects to one at a time, failing over to other Infranet Controllers in the cluster as required.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **interval on page 873**
- **timeout-action on page 886**
- *Junos OS Security Configuration Guide*

timeout-action

Syntax timeout-action (close | no-change | open):

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of Junos OS.

Description Specify what the SRX Series device should do when a timeout occurs and the device cannot connect to an Infranet Enforcer.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options **close**—Close existing sessions and block any further traffic. This is the default option.

no-change—Preserve existing sessions and require authentication for new sessions.

open—Preserve existing sessions and allow new sessions access.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- **interval on page 873**
- **timeout on page 885**
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

traceoptions (Application Identification Services)

Syntax

```
traceoptions {
   file filename <files number> <match regular-expression>
   <size maximum-file-size> <world-readable | no-world-readable>
   flag all;
   no-remote-trace;
}
```

Hierarchy Level [edit services application-identification]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configure tracing operations for application identification services.

Options

file ***filename***—By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files ***number***—(Optional) Specify the maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0,** then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match ***regular-expression*** —(Optional) Refine the output to include lines that contain the regular expression.

size ***maximum-file-size*** —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the **trace-file** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag all—Perform all tracing options for application identification services.

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

traceoptions (Unified Access Control)

Syntax

```
traceoptions {
  flag [ (ipc | config | connect | all) ];
}
```

Hierarchy Level
[edit services unified-access-control]

Release Information
Statement introduced in Release 9.4 of Junos OS.

Description
Define Unified Access Control (UAC) tracing options.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options
flag—Trace operation to perform. To specify more than one trace option, include multiple flag statements.

- **all**—Trace with all flags enabled
- **config**—Trace configuration information for all UAC-related configurations. This includes all configuration controlled through the **unified-access-control** statements at the **edit services** hierarchy level. It also includes other standard Junos OS configurations required for UAC enforcement such as zones, policies, and interfaces.
- **connect**—Trace communications between the Junos OS Enforcer and the Infranet Controller, including SSL handshakes and timeouts.
- **ipc**—Trace inter-process communications. Use this option to trace communications between the Routing Engine (RE) and the UACD enforcement plugin inside the Packet Forwarding Engine (PFE).

Required Privilege Level
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

unified-access-control

Syntax

```
unified-access-control {
  infranet-contoller hostname {
    address ip-address;
    port port-number;
    interface interface-name;
    password password;
    ca-profile ca-profile;
    server-certificate-subject subject;
  }
  timeout seconds;
  interval seconds;
  timeout-action (close | no-change | open):
test-only-mode (true | false):
  traceoptions {
    flag [ (ipc | config | connect | all) ];
  }
```

Hierarchy Level

[edit services]

Release Information

Statement introduced in Release 9.4 of Junos OS.

Description

Use this statement to configure the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 20

SNMP Hierarchy and Statements

This section contains the following topics:

- SNMP Configuration Statement Hierarchy on page 891

SNMP Configuration Statement Hierarchy

Use the statements in the **snmp** configuration hierarchy to configure the Simple Network Management Protocol (SNMP) for monitoring device operation and performance.

```
snmp {
  client-list list-name;
  community community-name {
    authorization (read-only | read-write);
    client-list-name client-list-name;
    clients {
      address < restrict>;
    }
    routing-instances routing-instances {
      client-list-name client-list-name ;
      clients {
        address < restrict>;
      }
    }
    view view-name ;
  }
  contact contact-information ;
  description description ;
  engine-id {
    (local engine-id | use-default-ip-address | use-mac-address);
  }
  filter-duplicates;
  health-monitor {
    falling-threshold percentage ;
    interval seconds;
    rising-threshold percentage ;
  }
  interface [ interface-names ];
  location location ;
  logical-system-trap-filter;
  name system-name ;
  nonvolatile {
```

```
    commit-delay seconds ;
  }
  rmon {
    alarm index {
      description description ;
      falling-event-index index ;
      falling-threshold integer ;
      falling-threshold-interval seconds ;
      interval seconds ;
      request-type (get-next-request | get-request | walk-request);
      rising-event-index index ;
      rising-threshold integer ;
      sample-type (absolute-value | delta-value);
      startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
      syslog-subtag text-string ;
      variable oid-variable ;
    }
    event index {
      community community-name ;
      description description ;
      type (log | log-and-trap | none | snmptrap);
    }
  }
  routing-instance access {
    access-list {
      routing-instance-name ;
    }
  }
  traceoptions {
    file filename <files number > <match regular-expression >
    <size maximum-file-size > <world-readable | no-world-readable>;
    flag flag ;
  }
  trap-group group-name {
    categories {
      authentication;
      chassis;
      configuration;
      link;
      remote-operations;
      rmon-alarm;
      routing;
      services;
      sonet-alarms {
        alarm-name ;
      }
      startup;
      vrrp-events;
    }
    destination-port port-number ;
    routing-instance instance-name ;
    targets {
    address ;
    }
    version (all | v1 | v2);
  }
```


Copyright © 2011, Juniper Networks, Inc.

```
trap-options {
  agent-address outgoing-interface;
  routing-instances instance-name {
    source-address address ;
  }
  source-address address ;
}
v3 {
  notify notify-name {
    tag tag-name ;
    type (inform | trap);
  }
  notify-filter notify-filter-name {
    oid oid-name <exclude | include>;
  }
  snmp-community community-index {
    community-name community-name ;
    context context ;
    security-name security-name ;
    tag tag-name ;
  }
  target-address target-address-name {
    address address ;
    address-mask address-mask ;
    port port-number ;
    retry-count number ;
    routing-instance instance-name ;
    tag-list tag-list ;
    target-parameters parameter-name ;
    timeout seconds ;
  }
  target-parameters target-parameters-name {
    notify-filter notify-filter-name ;{
      parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name ;
      }
    }
    usm {
      local-engine {
        user user-name {
          authentication-md5 {
            authentication-password password ;
          }
          authentication-none;
          authentication-sha {
            authentication-password password ;
          }
          privacy-3des {
            privacy-password password ;
          }
          privacy-aes128 {
            privacy-password password ;
          }
```

```
            privacy-des {
              privacy-password password ;
            }
            privacy-none;
          }
        }
        remote-engine {
          user user-name {
            authentication-md5 {
              authentication-password password ;
            }
            authentication-none;
            authentication-sha {
              authentication-password password ;
            }
            privacy-3des {
              privacy-password password ;
            }
            privacy-aes128 {
              privacy-password password ;
            }
            privacy-des {
              privacy-password password ;
            }
            privacy-none;
          }
        }
      }
      vacm {
        access {
          group group-name {
            context-prefix prefix {
              security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                  context-match (exact | prefix);
                  notify-view notify-view-name ;
                  read-view read-view-name ;
                  write-view write-view-name ;
                }
              }
            }
            default-context-prefix {
              security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                  context-match (exact | prefix);
                  notify-view notify-view-name ;
                  read-view read-view-name ;
                  write-view write-view-name ;
                }
              }
            }
          }
        }
        security-to-group {
          security-model (usm | v1 | v2c) {
            security-name security-name {
```


Copyright © 2011, Juniper Networks, Inc.

```
                group group-name ;
              }
            }
          }
        }
      }
      view view-name {
        oid oid-name {
          <exclude | include>;
        }
      }
    }
  }
```

Related Documentation

- *Junos OS Administration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

authorization

Syntax

authorization (read-only | read-write);

Hierarchy Level

[edit **snmp community** *community-name*]

Release Information

Statement modified in Release 8.5 of Junos OS.

Description

Set the access authorization for SNMP Get, GetBulk, GetNext, and Set requests.

Options

read-write—Enable all requests, including Set requests. You must configure a view to enable Set requests.

read-only—Enable Get, GetNext, and GetBulk requests. This is the default option.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

client-list-name

Syntax **client-list-name** *client-list-name* ;

Hierarchy Level [**edit snmp community** *community-name*]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration.

Options ***client-list-name*** — Name of the client list. Client list is the list of IP address prefixes defined with the **prefix-list** statement in the policy-options hierarchy.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

CHAPTER 21

SMTP Hierarchy and Statements

Use the statements in the **smtp** configuration hierarchy to configure Simple Mail Transfer Protocol (SMTP) to send an e-mail message to a local or a remote mail server to forward an e-mail message.

This chapter contains the following sections:

- SMTP Configuration Statement Hierarchy on page 897

SMTP Configuration Statement Hierarchy

```
smtp {
   primary-server {
   address IPv4 address;
   login sender-email {
   password password;
   }
}
secondary-server {
   address IPv4 address;
   login sender-email;
   password password ;
   }
}
traceoptions {
   flag flag ;
   }
}
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

flag

Syntax

```
traceoptions {
flag flag;
}
```

Hierarchy Level

[edit **smtp traceoptions flag**]

Release Information

Statement added in Release 10.0 of Junos OS.

Description

Set flag for the SMTP traceoptions.

Options

The following flag options are supported:

IPC—Trace inter-processs communication.

all—Trace everything.

configuration—Trace configuration event.

protocol-exchange—Trace SMTP protocol exchanges.

send-request—Trace send mail request event.

Required Privilege Level

SMTP—To view this statement in the configuration.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

primary-server

Syntax

```
primary-server {
address IPv4 address;
login sender-email {
password password;  }
}
```

Hierarchy Level [edit **smtp primary-server address**]

Release Information Statement added in Release 10.0 of Junos OS.

Description Set the access authorization for SMTP requests.

Options **address**—SMTP server's IPv4 address.

login—Configure a mail sender account to the server.

Required Privilege Level SMTP—To view this statement in the configuration.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

secondary-server

Syntax

```
secondary-server {
address IPv4 address;
login sender-email {
password password;
}
```

Hierarchy Level [edit **smtp secondary-server address**]

Release Information Statement added in Release 10.0 of Junos OS.

Description Set the access authorization for SMTP requests.

Options **address**—SMTP server's IPv4 address.

login—Configure a mail sender account to the server.

Required Privilege Level SMTP—To view this statement in the configuration.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

traceoptions

Syntax

```
traceoptions {
flag flag;
}
```

Hierarchy Level

[edit **smtp traceoptions**]

Release Information

Statement added in Release 10.0 of Junos OS.

Description

Set the SMTP traceoptions.

Options

apply-groups—Groups from which SMTP inherits configuration data.

apply-groups-except— Groups from which SMTP restricts inheriting configuration data from these groups.

Required Privilege Level

SMTP—To view this statement in the configuration.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS Network Management Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 22

System Hierarchy and Statements

This section includes the following topics:

- System Configuration Statement Hierarchy on page 901

System Configuration Statement Hierarchy

Use the statements in the **system** configuration hierarchy to configure system management functions including the device's hostname, address, and domain name; the addresses of the Domain Name System (DNS) servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; properties of the device's auxiliary and console ports; trace options; interface filtering; health monitoring; and many more features. Statement descriptions that are exclusive to the J Series and SRX Series devices running Junos OS are described in this chapter.

```
system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number ;
            retry number ;
            secret password ;
            source-address address ;
            timeout seconds ;
          }
        }
      }
      tacplus {
        server server-address {
          port port-number ;
          secret password ;
          single-connection;
          timeout seconds ;
        }
      }
    }
    events [login change-log interactive-commands];
    traceoptions {
```

```
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  archival {
    configuration {
      archive-sites {
        ftp:// < username >:< password >@< host >:< port >/< url-path >;
        scp: // < username >:< password >@< host >:< port >/< url-path >;
      }
      transfer-interval interval ;
      transfer-on-commit;
    }
  }
  arp {
    aging-timer minutes;
    passive-learning;
  }
  authentication-order [ authentication-methods ];
  autoinstallation {
    configuration-servers url {
      password password ;
    }
    interfaces interface-name {
      bootp;
      rarp;
      slarp;
    }
  }
  backup-router address <destination destination-address>;
  building name;
  commit synchronize;
  (compress-configuration-files | no-compression-configuration-files);
  default-address-selection;
  diag-port-authentication (encrypted-password "password" | plain-text-password);
  domain-name domain-name ;
  domain-search [ domain-list ];
  dump-device {
    boot-device;
    compact-flash;
    removable-compact-flash;
    usb;
  }
  encrypt-configuration-files;
  host-name hostname;
  inet6-backup-router address <destination destination-address >;
  internet-options address <destination destination-address >;
  internet-options {
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit {
      bucket-size seconds ;
      packet-rate packet-rate ;
    }
    icmpv6-rate-limit {
      bucket-size seconds ;
```


Copyright © 2011, Juniper Networks, Inc.

```
      packet-rate packet-rate ;
    }
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-quench;
    source-port upper-limit < upper-limit >;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
  }
  location {
    altitude feet ;
    building name ;
    country-code code ;
    floor number ;
    hcoord horizontal-coordinate ;
    lata service-area ;
    latitude degrees ;
    longitude degrees ;
    npa-nxx number ;
    postal-code postal-code ;
    rack number ;
    vcoord vertical-coordinate ;
  }
  login {
    announcement text ;
    class class-name {
      allow-commands " regular-expression ";
      allow-configuration " regular-expression ";
      deny-commands " regular-expression ";
      deny-configuration " regular-expression ";
      idle-timeout minutes ;
      login-alarms;
      login-tip;
      permissions [ permissions ];
    }
    message text ;
    password {
      change-type (set-transitions | character-set);
      format (md5 | sha1 | des);
      maximum-length length;
      minimum-changes number;
      minimum-length length;
    }
    user username {
      authentication {
        (encrypted-password "password"" | plain-text-password);
        ssh-dsa " public-key ";
        ssh-rsa " public-key ";
      }
      class class-name ;
      full-name complete-name ;
      uid uid-value ;
    }
    retry-options {
```

```
      backoff-threshold number ;
      backoff-factor seconds ;
      minimum-time seconds ;
      tries-before-disconnect number ;
    }
  }
  max-configurations-on-flash number ;
  mirror-flash-on-disk;
  name-server ip-address ;
  no-compress-configuration-files;
  no-multicast-echo;
  no-redirects;
  no-saved-core-context;
  ntp {
    authentication-key key-number type type value password ;
    boot-server (NTP) address ;
    broadcast < address > <key key-number > <version value > <ttl value >;
    broadcast-client;
    multicast-client < address >;
    peer address <key key-number > <version value > <prefer>;
    server address <key key-number > <version value > <prefer>;
    source-address source-address ;
    trusted-key [ key-numbers ];
  }
  pic-console-authentication {
    encrypted-password encrypted-password ;
    plain-text-password;
  }
  ports {
    auxiliary {
      disable;
      insecure;
      type terminal-type ;
    }
    console {
      disable;
      insecure;
      log-out-on-disconnect;
      type terminal-type ;
    }
  }
  processes {
    audit-process;
    bootp;
    chassis-control (enable | disable) failover failover-option;
    class-of-service (enable | disable) failover failover-option;
    craft-control (enable | disable) failover failover-option;
    dfc-daemon;
    dhcp (enable | disable) failover failover-option;
    dialer-services;
    disk-monitoring (enable | disable) failover failover-option;
    ecc-error-logging (enable | disable) failover failover-option;
    event-processing (enable | disable) failover failover-option;
    firewall (enable | disable) failover failover-option;
    firewall-authentication-service (enable | disable);
    forwarding;
```


Copyright © 2011, Juniper Networks, Inc.

```
general-authentication-service {
   (enable | disable);
   traceoptions {
      file filename {
         files number;
         match regular-expression;
         size maximum-file-size;
         <world-readable | no-world-readable>;
      }
      flag flag;
   }
}
ilmi;
inet-process (enable | disable) failover failover-option;
init;
interface-control (enable | disable) failover failover-option;
isdn-signaling;
kernel-replication (enable | disable) failover failover-option;
l2ald-service;
l2tp-service (enable | disable) failover failover-option;
lacp;
link-management (enable | disable) failover failover-option;
logical-system-mux;
mib-process (enable | disable) failover failover-option;
named;
network-security (enable | disable);
ntp (enable | disable) failover failover-option;
periodic-packet-services;
pfe;
pgm (enable | disable) failover failover-option;
pic-services-logging (enable | disable) failover failover-option;
ppp;
pppoe (enable | disable) failover failover-option;
redundancy-device (enable | disable) failover failover-option;
remote-operations (enable | disable) failover failover-option;
routing (enable | disable) failover failover-option;
sampling (enable | disable) failover failover-option;
service-deployment (enable | disable) failover failover-option;
snmp (enable | disable)  failover failover-option;
sonet-aps;
usb-control (enable | disable) failover failover-option;
vrrp;
watchdog (enable | disable) failover failover-option;
wan-acceleration {
   (enable | disable);
   traceoptions {
      file filename {
         files number;
         match regular-expression;
         size maximum-file-size;
         <world-readable | no-world-readable>;
      }
      flag flag;
   }
}
web-management (enable | disable) failover failover-option;
```

```
}
radius-options {
  attributes {
    nas-ip-address nas-ip-address ;
  }
}
radius-server server-address {
  accounting-port number ;
  port number ;
  retry number ;
  secret password ;
  source-address source-address ;
  timeout seconds ;
}
root-authentication {
  (encrypted-password " password " | plain-text-password);
  ssh-dsa " public-key ";
  ssh-rsa " public-key ";
}
(saved-core-context | no-saved-core-context);
saved-core-files number;
scripts {
  commit {
    allow-transients;
    file filename .xsl {
      optional;
      refresh;
      refresh-from url ;
      source url ;
    }
    refresh;
    refresh-from url ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  load-scripts-from-flash;
  op {
    file filename .xsl {
      arguments name {
        description cli-help-text ;
      }
      command filename-alias ;
      description cli-help-text ;
      refresh;
      refresh-from url ;
      source url ;
    }
    refresh;
    refresh-from url ;
    traceoptions {
      file filename <files number > <size maximum-file-size >;
      flag flag ;
    }
```


Copyright © 2011, Juniper Networks, Inc.

```
    }
  }
  services {
    dhcp {
      boot-file filename ;
      boot-server ( address | hostname );
      domain-name domain-name ;
      domain-search [ domain-list ];
      default-lease-time seconds;
      maximum-lease-time seconds;
      name-server {
        address ;
      }
      option {
        [ ( id-number option-type  option-value) | ( id-number array option-type
        option-values ) ];
      }
      pool {
        subnet-address ( address/netmask ) {
          address-range {
            high address;
            low address;
          }
          exclude-address {
            address ;
          }
        }
        propagate-settings propagate-settings;
      }
      propagate-settings propagate-settings;
      router {
        address ;
      }
      static-binding MAC-address {
        fixed-address {
          address ;
        }
        host hostname ;
        client-identifier (ascii client-id | hexadecimal client-id) ;
      }
      server-identifier address ;
      wins-server {
        address;
      }
    }
    dhcp-local-server {
      dhcpv6 {
        authentication {
          password password-string;
          username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            relay-agent-interface-id;
            relay-agent-remote-id;
```

```
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile {
      junos-default-profile;
      use-primary dynamic-profile-name-string;
    }
    group group-name {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name-string;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      dynamic-profile {
        junos-default-profile;
        use-primary dynamic-profile-name-string;
      }
      interface interface-name {
        exclude;
        overrides {
          interface-client-limit number;
        }
        trace;
        upto upto-interface-name;
      }
      overrides {
        interface-client-limit number;
      }
      reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
          radius-disconnect;
        }
      }
    }
    overrides {
      interface-client-limit number;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
```


Copyright © 2011, Juniper Networks, Inc.

```
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
}
duplicate-clients-on-interface;
forward-snooped-clients {
    all-interfaces;
    configured-interfaces;
    non-configured-interfaces;
}
interface-traceoptions {
    file filename {
        files number;
        match regular-expression;
        size maximum-file-size;
        <world-readable | no-world-readable>;
    }
    flag {
        all;
        dhcpv6-packet;
        dhcpv6-packet-option;
        dhcpv6-state;
        packet;
        packet-option;
        state;
    }
    no-remote-trace;
traceoptions {
    file filename {
        files number;
        match regular-expression;
        size maximum-file-size;
        <world-readable | no-world-readable>;
    }
    flag {
        all;
        auth;
        database;
        dhcpv6-general;
        dhcpv6-io;
        dhcpv6-packet;
        dhcpv6-packet-option;
        dhcpv6-rpd;
        dhcpv6-session-db;
        dhcpv6-state;
        fwd;
        general;
        ha;
        interface;
        io;
        packet;
        packet-option;
```

```
            performance;
            profile;
            rpd;
            rtsock;
            session-db
            state;
            statistics;
            ui;
        }
        no-remote-trace;
    }
    dns {
      dnssec {
        disable;
        dlv {
            domain-name domain-name {
                trusted-anchor trusted-anchor;
            }
        }
        secure-domains [domain-name];
        trusted-keys {
            key key;
            load-key-file {
                dns-keys;
            }
        }
      }
      forwarders ip-address;
      max-cache-ttl;
      max-ncache-ttl;
      traceoptions {
        category {
            category-type;
        }
        file;
      }
    }
    finger {
      <connection-limit limit >;
      <rate-limit limit >;
    }
    ftp {
      <connection-limit limit >;
      <rate-limit limit >;
    }
    netconf {
      ssh {
        <connection-limit number> ;
        <rate-limit number >;
      }
    }
    outbound-ssh {
      application-id application-id {
        device-id device-id ;
        ip-address {
            port port-number ;
```


Copyright © 2011, Juniper Networks, Inc.

```
        retry number ;
        timeout value ;
      }
      keep-alive number ;
      reconnect-strategy (in-order | sticky);
      secret secret ;
      services {
        netconf;
      }
    }
    traceoptions {
      file filename {
        <files number> ;
        <match regular-expression >;
        <size maximum-file-size >;
        <world-readable | no-world-readable>;
      }
      flag flag ;
    }
  }
  service-deployment {
    local-certificate certificate-name ;
    servers server-address {
      port-number port-number ;
    }
    source-address source-address ;
    traceoptions {
      flag flag ;
    }
  }
  ssh {
    <connection-limit limit >;
    protocol-version [v1 v2];
    <rate-limit limit >;
    root-login (allow | deny | deny-password);
  }
  telnet {
    <connection-limit limit >;
    <rate-limit limit >;
  }
  web-management {
    http {
      interface [ interface-name s];
      port port ;
    }
    https {
      interface [ interface-names ];
      local-certificate name ;
      pki-local-certificate name;
      port port ;
      system-generated-certificate;
    }
    session {
      idle-timeout [ minutes ];
      session-limit [ session-limit ];
    }
```

```
    }
    xnm-clear-text {
      connection-limit limit ;
      rate-limit limit ;
    }
    xnm-ssl {
      connection-limit limit ;
      local-certificate name ;
      rate-limit limit ;
    }
  }
  static-host-mapping hostname {
    alias [ alias ];
    inet [ address ];
    inet6 [address];
    sysid system-identifier ;
  }
  syslog {
    archive {
      archive-sites url;
      <files number >;
      <size maximum-file-size >;
      <world-readable | no-world-readable>;
    }
    console {
      facility severity ;
    }
    file filename {
      facility severity ;
      explicit-priority;
      match " regular-expression ";
      archive {
        files number ;
        size maximum-file-size ;
        start-time;
        transfer-interval;
        <world-readable | no-world-readable>;
      }
    }
    host ( hostname | other-routing-engine | scc-master) {
      any;
      authorization;
      change-log;
      conflict-log;
      daemon;
      dfc;
      external;
      firewall;
      ftp;
      interactive-commands;
      kernel;
      pfe;
      user;
      explicit-priority;
      facility-override facility ;
      log-prefix string ;
```


Copyright © 2011, Juniper Networks, Inc.

```
        match " regular-expression ";
      }
      source-address source-address {
        archive;
        console;
        file;
        host;
        time-format;
        user;
      }
      time-format (year | millisecond | year millisecond);
      user ( username | *) {
        match < regular-expression >;
      }
    }
    tacplus-options service-name service-name ;
    tacplus-server server-address {
      port port-number;
      secret password ;
      single-connection;
      source-address source-address ;
      timeout seconds ;
    }
    time-zone (GMT hour-offset | time-zone );
  }
```

Related Documentation

- *Junos OS Administration Guide for Security Devices*
- *Junos OS Security Configuration Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- *Junos OS System Basics Configuration Guide*
- *Junos OS Network Management Configuration Guide*

dhcpv6

Syntax

```
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile {
    junos-default-profile;
    use-primary dynamic-profile-name-string;
  }
  group group-name {
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile {
      junos-default-profile;
      use-primary dynamic-profile-name-string;
    }
    interface interface-name {
      exclude;
      overrides {
        interface-client-limit number;
      }
      trace;
      upto upto-interface-name;
    }
    overrides {
      interface-client-limit number;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
```


Copyright © 2011, Juniper Networks, Inc.

```
            strict;
            timeout number;
            token token-name;
            trigger {
              radius-disconnect;
            }
          }
        }
        overrides {
          interface-client-limit number;
        }
        reconfigure {
          attempts number;
          clear-on-abort;
          strict;
          timeout number;
          token token-name;
          trigger {
            radius-disconnect;
          }
        }
      }
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure DHCPv6 server to provide IPv6 addresses to clients.

NOTE: SRX and J series devices do not support client authentication.

Options

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

dhcp-local-server (dhcpv6)

Syntax

```
dhcp-local-server {
  dhcpv6 {
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile {
      junos-default-profile;
      use-primary dynamic-profile-name-string;
    }
    group group-name {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name-string;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      dynamic-profile {
        junos-default-profile;
        use-primary dynamic-profile-name-string;
      }
      interface interface-name {
        exclude;
        overrides {
          interface-client-limit number;
        }
        trace;
        upto upto-interface-name;
      }
      overrides {
        interface-client-limit number;
      }
      reconfigure {
        attempts number;
```


Copyright © 2011, Juniper Networks, Inc.

```
            clear-on-abort;
            strict;
            timeout number;
            token token-name;
            trigger {
                radius-disconnect;
            }
        }
    }
    overrides {
        interface-client-limit number;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
}
duplicate-clients-on-interface;
forward-snooped-clients {
    all-interfaces;
    configured-interfaces;
    non-configured-interfaces;
}
interface-traceoptions {
    file filename {
        files number;
        match regular-expression;
        size maximum-file-size;
        <world-readable | no-world-readable>;
    }
    flag {
        all;
        dhcpv6-packet;
        dhcpv6-packet-option;
        dhcpv6-state;
        packet;
        packet-option;
        state;
    }
    no-remote-trace;
traceoptions {
    file filename {
        files number;
        match regular-expression;
        size maximum-file-size;
        <world-readable | no-world-readable>;
    }
    flag {
        all;
        auth;
```

```
        database;
        dhcpv6-general;
        dhcpv6-io;
        dhcpv6-packet;
        dhcpv6-packet-option;
        dhcpv6-rpd;
        dhcpv6-session-db;
        dhcpv6-state;
        fwd;
        general;
        ha;
        interface;
        io;
        packet;
        packet-option;
        performance;
        profile;
        rpd;
        rtsock;
        session-db
        state;
        statistics;
        ui;
      }
      no-remote-trace;
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.

NOTE: SRX and J Series devices do not support client authentication.

Options

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

disable (dnssec)

Syntax **disable**

Hierarchy Level **[edit system services dns dnssec]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Disables DNSSEC in the DNS server.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

dlv

Syntax

```
dlv {
   domain-name domain-name {
      trusted-anchor trusted-anchor;
   }
}
```

Hierarchy Level **[edit system services dns dnssec]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configures DNS Lookaside Validation (DLV) in the DNS server.

Options **domain-name**—Name of the domain.

trusted-anchor—Name of the trusted DLV anchor.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

dns

Syntax

```
dns {
  dnssec {
    disable;
    dlv {
      domain-name domain-name {
        trusted-anchor trusted-anchor;
      }
    }
    secure-domains [domain-name];
    trusted-keys {
      key key;
      load-key-file {
        dns-keys;
      }
    }
  }
  forwarders ip-address;
  max-cache-ttl;
  max-ncache-ttl;
  traceoptions {
    category {
      category-type;
    }
    file;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configures the DNS server.

Options

dnssec—This option is explained separately.

forwarders—This option is explained separately.

max-cache-ttl—Maximum time-to-live (TTL) for cached responses, in seconds. The configurable range varies from 0 through 604800 seconds.

max-ncache-ttl—Maximum time-to-live (TTL) for cached negative responses, in seconds. The configurable range varies from 0 through 604800 seconds.

traceoptions—DNS server trace options. This option is explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

dnssec

Syntax

```
dnssec {
  disable;
  dlv {
    domain-name domain-name {
      trusted-anchor trusted-anchor;
    }
  }
  secure-domains [domain-name];
  trusted-keys {
    key key;
    load-key-file {
    dns-keys;
    }
  }
}
```

Hierarchy Level **[edit system services dns]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configures DNSSEC in the DNS server.

Options The options are explained separately

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

firewall-authentication-service

Syntax firewall-authentication-service (enable | disable);

Hierarchy Level **[edit system processes]**

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable or disable the firewall authentication service process.

Options **enable**—Start the firewall authentication service process.

disable—Stop the firewall authentication service process.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

forwarders

Syntax forwarders *ip-address*;

Hierarchy Level [edit system services dns]

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configures a DNS server to act as a forwarder. When a DNS server cannot resolve a query, it forwards the query requests to the DNS server that is configured as a forwarder.

Options ***ip-address***—IP address of the DNS server that acts as a forwarder.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

general-authentication-service

Syntax

```
general-authentication-service {
  (enable | disable);
  traceoptions {
    file filename {
      <files number >;
      <match regular-expression>;
      <size maximum-file-size>;
      <world-readable | no-world-readable>;
    }
    flag flag ;
  }
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable or disable the general authentication process.

Options **enable**—Start the general authentication service process.

disable—Stop the general authentication service process.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

group (DHCP Local Server)

Syntax

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile {
    junos-default-profile;
    use-primary dynamic-profile-name-string;
  }
  interface interface-name {
    exclude;
    overrides {
      interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
  }
  overrides {
    interface-client-limit number;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
}
```

Hierarchy Level [edit system services dhcp-local-server dhcpv6]

Release Information Statement introduced in Release 10.4 of Junos OS.

Description Configure a group of interfaces that have a common configuration. The remaining statements are explained separately.

Options

- *group-name*—Name of the group.

NOTE: SRX and J Series devices do not support DHCP client authentication.

Required Privilege Level
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

interface (DHCP Local Server)

Syntax

```
interface interface-name {
   exclude;
   overrides {
      interface-client-limit number;
   }
   trace;
   upto upto-interface-name;
}
```

Hierarchy Level
[edit system services dhcp-local-server dhcpv6 group*group-name*]

Release Information
Statement introduced in Release 10.4 of Junos OS.

Description
Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

Options
- *interface-name*—Name of the interface.
- **trace**—Enables tracing of the interface specified by the *interface-name* argument.
- **upto** *upto-interface-name*—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the *upto-interface-name* must be the same as the device name of the *interface-name*.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

interface-traceoptions (DHCP Local Server)

Syntax

```
interface-traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level

[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the **interface** ***interface-name*** **trace** statement at the **[edit system services group** ***group-name*****]** hierarchy level to enable the tracing operation on the specific interfaces.

Options

file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (“ ”). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files ***number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag ***flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **packet**—Trace packet decoding operations
- **packet-option**—Trace DHCP option decoding operations
- **state**—Trace changes in state

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

network-security

Syntax
network-security (enable | disable);

Hierarchy Level
[edit system processes]

Release Information
Statement introduced in Release 8.5 of Junos OS.

Description
Enable or disable the network security process on the device.

Options
enable—Start the network security process.

disable—Stop the network security process.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

overrides (DHCP Local Server)

Syntax

```
overrides {
   interface-client-limit number
}
```

Hierarchy Level

[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server dhcpv6 group *group-name*]
[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Override the default configuration settings for the extended DHCP local server. Specifying the **overrides** statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the **[edit system services dhcp-local-server]** hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name*]** hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*]** hierarchy level.
- Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.

Options

interface-client-limit *number*—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Range: 1 through 500,000

Default: No limit

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

pki-local-certificate

Syntax pki-local-certificate *name* ;

Hierarchy Level [edit system services web-management https]

Release Information Statement introduced in Release 9.1 of Junos OS.

Description Specify the name of the certificate that is generated by public key infrastructure (PKI) and authenticated by certificate authority (CA).

Options *name* —Name of certificate.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

propagate-settings

Syntax propagate-settings *logical-interface-name* ;

Hierarchy Level [edit system services dhcp],
[edit system services dhcp pool]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable or disable the propagation of TCP/IP settings received on the device acting as Dynamic Host Configuration Protocol (DHCP) client. The settings can be propagated to the server pool running on the device. Use the **system services dhcp** statement to set this feature globally. Use the **system services dhcp pool** statement to set the feature for the address pool and override the global setting.

Options *logical-interface-name* —Name of the logical interface to receive TCP/IP settings from the external network for propagation to the DHCP pool running on the device.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

reconfigure (DHCP Local Server)

Syntax

```
reconfigure {
   attempts number;
   clear-on-abort ;
   strict ;
   timeout seconds;
   token token-name;
}
```

Hierarchy Level

[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server group *group-name*]
[edit system services dhcp-local-server dhcpv6 group *group-name*]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.

Options

attempts *number*—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 attempts

Default: 8 attempts

clear-on-abort —Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

strict —Configure the system to only allow packets that contain the reconfigure accept option.

timeout *seconds*—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempts doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 seconds

Default: 2 seconds

token *token-name*—Configures a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

reverse ssh

Syntax reverse ssh

Hierarchy Level [edit system services reverse ssh]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. Use reverse SSH to encrypt the reverse Telnet communication between the device and the client.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

reverse ssh port

Syntax reverse ssh port *5000*

Hierarchy Level [edit system services reverse ssh port 5000]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Reverse SSH allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2901 is used.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

reverse telnet

Syntax reverse telnet

Hierarchy Level [edit system services reverse telnet]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

reverse telnet port

Syntax reverse telnet port *6000*

Hierarchy Level [edit system services reverse telnet port 6000]

Release Information Statement introduced in Release 9.6 of Junos OS.

Description Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2900 is used.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Administration Guide for Security Devices*

secure-domains

Syntax secure-domains [*domain-name*];

Hierarchy Level **[edit system services dns dnssec]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Configures secure domains in the DNS server. The server accepts only signed responses for this domain. For unsigned responses, the server returns SERVFAIL error to the client.

Options **domain-name**—Name of the domain.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

system-generated-certificate

Syntax system-generated-certificate;

Hierarchy Level [edit system services web-management https]

Description Automatically generated self-signed certificate

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Security Configuration Guide*

 Copyright © 2011, Juniper Networks, Inc.

traceoptions (DHCP Local Server)

Syntax

```
traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level

[edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information

Statement introduced in Release 10.4 of Junos OS.

Description

Configure extended DHCP local server tracing operations for DHCP processes.

Options

file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (“ ”). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

no-world-readable—(Optional) Disable unrestricted file access.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events.
- **database**—Trace database operations.
- **dhcpv6-general**—Trace operations for DHCPv6.
- **dhcpv6-io**—Trace input/output operations for DHCPv6.

- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-rpd**—Trace routing protocol process operations.
- **dhcpv6-session-db**—Trace session database operations for DHCPv6.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **fwd**—Trace firewall process operations.
- **general**—Trace miscellaneous general operations.
- **ha**—Trace high-availability related operations.
- **interface**—Trace interface operations.
- **io**—Trace input/output operations.
- **packet**—Trace packet decoding operations.
- **packet- option**—Trace DHCP option decoding operations.
- **performance**—Trace DHCP performance measurement operations.
- **profile**—Trace DHCP profile operations.
- **rpd**—Trace routing protocol process operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace changes in statistics.
- **ui**—Trace changes in user interface operations.

no remote-trace—Disable remote tracing.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Administration Guide for Security Devices*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (dns)

Syntax

```
traceoptions {
   category {
      category-type;
   }
   file;
}
```

Hierarchy Level **[edit system services dns]**

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Defines tracing options for DNS services.

Options **category**—Specifies the logging category. See Table 6 on page 936 for the different logging categories and their descriptions.

file—Trace file information.

Table 6: Category Names

Category Name	Description
client	Processing of client requests
config	Configuration file parsing and processing
database	Messages relating to the databases
default	Categories for which there is no specific configuration
delegation-only	Delegation only
dispatch	Dispatching of incoming packets to the server
dnssec	DNSSEC and TSIG protocol processing
edns-disabled	Log query using plain DNS
general	General information
lame-servers	Lame servers
network	Network options
notify	NOTIFY protocol
queries	DNS query resolver
resolver	DNS resolution security
security	Approval and denial of requests
unmatched	Unable to determine the class for messages named
update	Dynamic updates
update-security	Approval and denial of update requests
xfer-in	Zone transfers that the server is receiving xfer-out
xfer-out	Zone transfers that the server is sending

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

traceoptions (General Authentication Service)

Syntax

```
traceoptions {
  file filename {
    <files number>;
    <match regular-expression>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit system processes general-authentication-service]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure tracing operations for general-authentication-service processes.

Options

file *filename* —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files *number* —(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag* —Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all** —Trace with all flags enabled
  - **configuration** —Trace configuration events
  - **framework**—Trace authentication framework events
  - **ldap** —Trace ldap authentication events
  - **local-authentication**—Trace local authentication events
  - **radius** —Trace radius authentication events

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

traceoptions (WAN Acceleration)

Syntax

```
traceoptions {
  file filename {
    <files number> ;
    <match regular-expression>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

Hierarchy Level [edit *system* **processes** wan-acceleration]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Configure tracing operations for WXC Integrated Services Module (ISM 200) processes.

Options

file *filename* —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

files *number* —(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag* —Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all**—Trace all options
  - **configuration** — Trace configuration events
  - **fpc-ipc**—Trace FPC interprocess communication messages
  - **fpc-ipc-heart-beat**—Trace FPC interprocess heart beat messages
  - **memory**—Trace memory allocation or deallocation messages
  - **ssam**—Trace state synchronization and management events
  - **wx-login**—Trace WXC ISM200 login events

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- *WXC Integrated Services Module Installation and Configuration Guide*

trusted-keys

Syntax

```
trusted-keys {
   key dns-key;
   load-key-file {
   load-key-file;
   }
}
```

Hierarchy Level

[edit system services dns dnssec]

Release Information

Statement introduced in Release 10.2 of Junos OS.

Description

Configures trusted keys in the DNS server.

Options

key ***dns-key***—Trusted key

load-key-file ***load-key-file***—Specifies the URL containing the DNS keys.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Security Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

wan-acceleration

Syntax wan-acceleration (enable | disable);

Hierarchy Level [edit system processes]

Release Information Statement introduced in Release 8.5 of Junos OS.

Description Enable or disable the WXC Integrated Services Module (ISM 200) for WAN acceleration.

Options **enable**—Turn on the WXC ISM200.

disable—Turn off the WXC ISM200.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *WXC Integrated Services Module Installation and Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 23

WLAN Hierarchy and Statements

This section contains the following topics:

- [edit wlan] Configuration Statement Hierarchy on page 943

[edit wlan] Configuration Statement Hierarchy

Use the statements in the **wlan** configuration hierarchy to configure wireless LAN features on the SRX210, SRX240, and SRX650 Services Gateways running Junos OS.

```
wlan {
  access-point name {
    description description;
    access-point-options {
      country country-code;
      station-mac-filter {
        ( allow-list | deny-list );
        mac-address addr1 addr2 ... addrn;
      }
    }
    cluster {
      ID
    }
    external {
      dot1x-supplicant {
        username username;
        password password;
      }
      system {
        console {
          baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
        }
        ntp-server name;
        ports {
          ethernet {
            management-vlan vlan-id;
            name-server {
              ip-address1 ip-address2;
            }
            static {
              address ip-address/mask;
              default-gateway ip-address;
```

```
            }
            untagged-vlan vlan-id;
          }
        }
      }
    }
    location location;
    logging-options {
      enable-persistent;
      enable-remote;
      log-server-address <ip-address>;
      log-server-port <port-number>;
    }
    mac-address mac-address;
    radio ( 1 | 2 ){
      quality-of-service {
        access-point-queues {
          background-queue {
            arbitration-inter-frame-space slots;
            maximum-burst microseconds;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          }
          best-effort-queue {
            arbitration-inter-frame-space slots;
            maximum-burst microseconds;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          }
          video-queue {
            arbitration-inter-frame-space slots;
            maximum-burst microseconds;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          }
          voice-queue {
            arbitration-inter-frame-space slots;
            maximum-burst microseconds;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          }
        }
        no-acknowledgement;
        no-auto-power-save;
        no-wifi-multimedia;
        station-queues {
          background-queue {
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
          }
          best-effort-queue {
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
```


Copyright © 2011, Juniper Networks, Inc.

```
            transmit-opportunity-limit ms;
        }
        video-queue {
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        voice-queue {
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
radio-options {
    beacon-interval ms;
    broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
    }
    channel {
        number ( auto | channel-number );
        bandwidth (20 | 40 );
        primary ( lower | upper );
    }
    disable-dot11d;
    dtim-period beacons;
    fixed-multicast-rate ( auto | rate );
    fragmentation-threshold size;
    maximum-stations number;
    mode (2.4GHz | 5GHz | a | an | bg | bgn);
    protection ( auto | off );
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
        supported-rates rate1 rate2 ... rate-n;
        supported-basic-rates rate1 rate2 ... rate-n;
    }
}
virtual-access-point id {
    description description;
    http-redirect {
        redirect-url url;
    }
    no-broadcast-ssid;
    security {
        dot1x {
            radius-server ip-address;
            radius-key secret-key;
            broadcast-key-refresh-rate minutes;
            session-key-refresh-rate minutes;
        }
```

```
                mac-authentication-type ( disabled | local | radius );
                none;
                static-wep {
                    authentication-type (open | shared | both);
                    key-length (64bits | 128bits);
                    key-type ( ascii | hex );
                    transfer-key-index id;
                    wep-key-1 key-1;
                    wep-key-2 key-2;
                    wep-key-3 key-3;
                    wep-key-4 key-4;
                }
                wpa-enterprise {
                    cipher-suites (tkip | ccmp | both);
                    pre-authenticate;
                    radius {
                        radius-server ip-address;
                        radius-key secret-key;
                        broadcast-key-refresh-rate minutes;
                        session-key-refresh-rate minutes;
                    }
                    wpa-version (v1 | v2 | both);
                }
                wpa-personal {
                    broadcast-key-refresh-rate minutes;
                    cipher-suites (tkip | ccmp | both);
                    key key;
                    wpa-version (v1 | v2 | both);
                }
            }
            ssid ssid;
            vlan vlan-id;
        }
    }
    syslog-options {
        log-size <number>;
        period <number>;
    }
}
    cluster ID {
        name;
            logging-options {
                enable-persistent;
                enable-remote;
                log-server-address <ip-address>;
                log-server-port <port-number>;
            }
default-cluster;
    interfaces;
    channel-management;
    access-point-options {
        country country-code;
        disable-dot11d ;
        station-mac-filter {
            action ( allow | deny );
            mac-address addr1 addr2 ... addrn;
```


Copyright © 2011, Juniper Networks, Inc.

```
    }
  }
  radio ( 1 | 2 ) {
    radio-options {
      beacon-interval ms;
      broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
      }
      channel {
        number ( auto | channel-number );
        bandwidth (20 MHz | 40 MHz );
        primary-channel ( lower | upper );
      }
      dtim-period beacons;
      fixed-multicast-rate ( auto | rate );
      fragmentation-threshold size;
      max-stations number;
      mode ( a | bg | an | bgn | 5GHz-n | 2.4GHz-n );
      no-short-guard-interval-supported;
      protection ( auto | off );
      radio-off;
      rts-threshold size;
      space-time-block-coding;
      transmit-power percent;
      transmit-rate-sets {
        supported-rates rate1 rate2 ... rate-n;
        supported-basic-rates rate1 rate2 ... rate-m;
      }
    }
    quality-of-service {
      access-point-queues {
        background-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst ms;
        }
        best-effort-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst ms;
        }
        video-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst ms;
        }
        voice-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst ms;
        }
```

```
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      voice-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
    }
  }
  virtual-access-point id {
    description description;
    http-redirect {
      redirect-url url;
    }
    no-broadcast-ssid;
    security {
      mac-authentication-type ( disabled | local | radius );
      none;
      dot1x {
        radius {
          radius-server ip-address;
          radius-key secret-key;
          broadcast-key-refresh-rate minutes;
          session-key-refresh-rate minutes;
        }
      }
      static-wep {
        authentication-type ( open | shared );
        key-length ( 64-bit | 128-bit );
        key-type ( ascii | hex );
        transfer-key-index id;
        wep-key-1 key-1;
        wep-key-2 key-2;
        wep-key-3 key-3;
```


Copyright © 2011, Juniper Networks, Inc.

```
                wep-key-4 key-4;
              }
              wpa-enterprise {
                wpa-version ( 1 | 2 | both );
                cipher-suites (tkip | ccmp | both );
                pre-authenticate;
                radius {
                  radius-server ip-address;
                  radius-key secret-key;
                  broadcast-key-refresh-rate minutes;
                  session-key-refresh-rate minutes;
                }
              }
              wpa-personal {
                wpa-version ( 1 | 2 | both );
                cipher-suites ( tkip | ccmp | both );
                key key;
                broadcast-key-refresh-rate minutes;
              }
            }
            ssid ssid;
            vlan vlan-id;
          }
        }
      }
    }
```

Related Documentation

- *Junos OS WLAN Configuration and Administration Guide*

access-point

Syntax

```
access-point name {
  access-point-options {
    country country-code;
    station-mac-filter {
      ( allow-list | deny-list );
      mac-address addr1 addr2 ... addrn;
    }
  }
  description description;
  external {
    dot1x-supplicant {
      username username;
      password password;
    }
    system {
      console {
        baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
      }
      ntp-server name;
      ports {
        ethernet {
          management-vlan vlan-id;
          name-server {
            ip-address1 ip-address2;
          }
          static {
            address ip-address/mask;
            default-gateway ip-address;
          }
          untagged-vlan vlan-id;
        }
      }
    }
  }
  location location;
  mac-address mac-address;
  radio ( 1 | 2 ){
    quality-of-service {
      access-point-queues {
        background-queue {
          arbitration-inter-frame-space slots;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst microseconds;
        }
        best-effort-queue {
          arbitration-inter-frame-space slots;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst microseconds;
        }
        video-queue {
```


Copyright © 2011, Juniper Networks, Inc.

```
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-burst microseconds;
        }
        voice-queue {
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-burst microseconds;
        }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
        background-queue {
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        best-effort-queue {
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        video-queue {
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        voice-queue {
            arbitration-inter-frame-space slots;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
radio-options {
    beacon-interval ms;
    broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
    }
    channel {
        number ( auto | channel-number );
        bandwidth (20 | 40 );
        primary ( lower | upper );
    }
    disable-dot11d;
    dtim-period beacons;
    fixed-multicast-rate ( auto | rate );
```

```
    fragmentation-threshold size;
    maximum-stations number;
    mode (2.4GHz | 5GHz | a | an | bg | bgn);
    no-short-guard-interval-supported;
    protection ( auto | off );
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
      supported-rates rate1 rate2 ... rate-n;
      supported-basic-rates rate1 rate2 ... rate-n;
    }
  }
  virtual-access-point id {
    description description;
    http-redirect {
      redirect-url url;
    }
    no-broadcast-ssid;
    security {
      dot1x {
        radius-server ip-address;
        radius-key secret-key;
        broadcast-key-refresh-rate minutes;
        session-key-refresh-rate minutes;
      }
      mac-authentication-type ( disabled | local | radius );
      none;
      static-wep {
        authentication-type (open | shared | both);
        key-length (64bits | 128bits);
        key-type ( ascii | hex );
        transfer-key-index id;
        wep-key-1 key-1;
        wep-key-2 key-2;
        wep-key-3 key-3;
        wep-key-4 key-4;
      }
      wpa-enterprise {
        cipher-suites (tkip | ccmp | both);
        pre-authenticate;
        radius {
          radius-server ip-address;
          radius-key secret-key;
          broadcast-key-refresh-rate minutes;
          session-key-refresh-rate minutes;
        }
        wpa-version (v1 | v2 | both);
      }
      wpa-personal {
        broadcast-key-refresh-rate minutes;
        cipher-suites (tkip | ccmp | both);
        key key;
        wpa-version (v1 | v2 | both);
      }
```

 Copyright © 2011, Juniper Networks, Inc.

```
            }
            ssid ssid;
            vlan vlan-id;
        }
    }
}
```

Hierarchy Level [edit wlan]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure WLAN access points.

Options **access-point**—Name of the access point. Enter a string of up to 20 characters. The name must start with a letter and end with a letter or a number. Only letters, numbers, and dashes are allowed.

description—Descriptive text about the access point.

location—Descriptive text about the location of the access point.

mac-address—MAC address of the Ethernet port on the access point.

NOTE: The MAC address uniquely identifies the access point and must be configured before you can change the default configuration of the access point.

If the access point is connected to the SRX Series device and powered on, the MAC address is displayed with the **show wlan access-points** or **show wlan access-points *ap-name* detail** operational mode commands.

The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

access-point-options

Syntax

```
access-point-options {
   country country-code;
   station-mac-filter {
      ( allow-list | deny-list );
      mac-address addr1 addr2 ... addrn;
   }
}
```

Hierarchy Level [edit wlan access-point *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure access point options.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

access-point-queues

Syntax

```
access-point-queues {
  background-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  best-effort-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  video-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  voice-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure enhanced distributed channel access (EDCA) parameters for downstream traffic from the access point to the client for the following queues:

Options Options can be configured for the following queues:

- **voice-queue**—Highest priority queue with minimum delay.
- **video-queue**—High priority queue with minimum delay.
- **best-effort-queue**—Medium priority queue with medium throughput and delay.
- **background-queue**—Lowest priority queue with high throughput.

The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

arbitration-inter-frame-space

Syntax arbitration-inter-frame-space *slots*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure wait time, in number of slots, for data frames. The length of a slot time is a constant that depends on the physical characteristics of the 802.11 PHY.

Options **arbitration-inter-frame-space**—Specify a value from 1 to 255. The defaults are 2 slots for **voice-queue** and **video-queue**, 3 slots for **best-effort-queue**, and 7 slots for **background-queue**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

background-queue

Syntax For access-point-queues:

```
background-queue {
  arbitration-inter-frame-space slots;
  maximum-burst microseconds;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
background-queue {
  arbitration-inter-frame-space slots;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  transmit-opportunity-limit ms;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure lowest priority queue with high throughput.

Options The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

 Copyright © 2011, Juniper Networks, Inc.

beacon-interval

Syntax beacon-interval *ms*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure interval, in milliseconds, at which the radio transmits beacons.

Options **beacon-interval**—Specify a value from 20 to 2000. The default is 100 milliseconds.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

best-effort-queue

Syntax For access-point-queues:

```
best-effort-queue {
   arbitration-inter-frame-space slots;
   maximum-burst microseconds;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
best-effort-queue {
   arbitration-inter-frame-space slots;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   transmit-opportunity-limit ms;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure medium priority queue with medium throughput and delay.

Options The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

broadcast-multicast-rate-limit

Syntax

```
broadcast-multicast-rate-limit {
   rate-limit packets-per-second;
   rate-limit-bursts packets-per-second;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable broadcast and multicast rate limiting.

Options

rate-limit—Packet rate, in packets per second, below which frames are forwarded. Specify a value from 1 to 50. The default is 50 packets per second.

rate-limit-bursts—Intermittent packet burst rate, in packets per second, below which frames are forwarded. Specify a value from 1 to 75. The default is 75 packets per second.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

channel

Syntax

```
channel {
   number ( auto | channel-number );
   bandwidth (20 | 40 );
   primary ( lower | upper );
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure channel used for transmitting and receiving.

Options

number—Specify a valid 802.11a/b/g channel number or **auto**.

bandwidth —Channel bandwidth to be used. Specify **20** for the 2.4 GHz band or **40** for the 5 GHz band.

primary—In the 40 MHz channel, the relative location of the primary channel. Specify **lower** or **upper**.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

channel-management

Syntax channel-management;

Hierarchy Level [edit wlan cluster *ID*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description (Optional) Enable channel management among the access points in the cluster.

Options ***ID***—ID of the access point cluster. Enter a string of up to 64 characters.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

cluster

Syntax

```
cluster ID {
  name;
  default-cluster;
  interfaces;
  channel-management;
  access-point-options {
    country country-code;
    disable-dot11d;
    station-mac-filter {
      action ( allow | deny );
      mac-address addr1 addr2 ... addrn;
    }
  }
  radio ( 1 | 2 ){
    radio-options {
      beacon-interval ms;
      broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
      }
      channel {
        number ( auto | channel-number );
        bandwidth (20 MHz | 40 MHz );
        primary-channel ( lower | upper );
      }
      dtim-period beacons;
      fixed-multicast-rate ( auto | rate );
      fragmentation-threshold size;
      max-stations number;
      mode ( a | bg | an | bgn | 5GHz-n | 2.4GHz-n );
      no-short-guard-interval-supported;
      protection ( auto | off );
      radio-off;
      rts-threshold size;
      space-time-block-coding;
      transmit-power percent;
      transmit-rate-sets {
        supported-rates rate1 rate2 ... rate-n;
        supported-basic-rates rate1 rate2 ... rate-m;
      }
    }
    quality-of-service {
      access-point-queues {
        background-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst ms;
        }
        best-effort-queue {
          arbitration-inter-frame-space ms;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
```


Copyright © 2011, Juniper Networks, Inc.

```
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-burst ms;
        }
        video-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-burst ms;
        }
        voice-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-burst ms;
        }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
        background-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        best-effort-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        video-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
        voice-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
virtual-access-point id {
    description description;
    http-redirect {
        redirect-url url;
    }
    no-broadcast-ssid;
    security {
        mac-authentication-type ( disabled | local | radius );
        none;
        dot1x {
```

```
                radius {
                    radius-server ip-address;
                    radius-key secret-key;
                    broadcast-key-refresh-rate minutes;
                    session-key-refresh-rate minutes;
                }
            }
            static-wep {
                authentication-type ( open | shared );
                key-length ( 64-bit | 128-bit );
                key-type ( ascii | hex );
                transfer-key-index id;
                wep-key-1 key-1;
                wep-key-2 key-2;
                wep-key-3 key-3;
                wep-key-4 key-4;
            }
            wpa-enterprise {
                wpa-version ( 1 | 2 | both );
                cipher-suites (tkip | ccmp | both);
                pre-authenticate;
                radius {
                    radius-server ip-address;
                    radius-key secret-key;
                    broadcast-key-refresh-rate minutes;
                    session-key-refresh-rate minutes;
                }
            }
            wpa-personal {
                wpa-version ( 1 | 2 | both );
                cipher-suites ( tkip | ccmp | both );
                key key;
                broadcast-key-refresh-rate minutes;
            }
        }
        ssid ssid;
        vlan vlan-id;
    }
  }
}
```

Hierarchy Level [edit wlan]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Configure access point cluster.

Options *name*—Name of the access point cluster. Enter a string of up to 64 characters.

channel-management—Enable channel management.

The remaining statements are explained separately.

 Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

cluster (access point)

Syntax
cluster *ID*;

Hierarchy Level
[edit wlan access-point *name*]

Release Information
Statement introduced in Release 10.1 of Junos OS.

Description
Assign access point to cluster.

Options
ID—ID of the access point cluster. Enter a string of up to 64 characters.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

console

Syntax

```
console {
  baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
}
```

Hierarchy Level
[edit wlan access-point *name* external system]

Release Information
Statement introduced in Release 10.0 of Junos OS.

Description
Configure serial access on the access point's console port.

Options
console—Enable serial access on access point's console port. Console port access is disabled by default.

Specify the baud rate for the serial connection: **9600**, **19200**, **38400**, **57600**, or **115200**.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

country

Syntax country *country-code*;

Hierarchy Level [edit wlan access-point *name* access-point-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure country of operation for the access point.

Options **country**—Two-character code that represents the country of operation for the access point. The following lists supported countries and their country codes:

- Australia—AU
- Austria—AT
- Belgium—BE
- Brazil—BR
- Canada—CA
- China—CN
- Czech Republic—CZ
- Denmark—DK
- Finland—FI
- France—FR
- Germany—DE
- Greece—GR
- Hong Kong—HK
- Hungary—HU
- Iceland—IS
- India—IN
- Ireland—IE
- Israel—IL
- Italy—IT
- Japan—JP
- Liechtenstein—LI
- Luxembourg—LU
- Malaysia—MY
- Mexico—MX

Copyright © 2011, Juniper Networks, Inc.

- Netherlands—NL
- New Zealand—NZ
- Norway—NO
- Poland—PL
- Portugal—PT
- Saudi Arabia—SA
- Singapore—SG
- Slovakia—SK
- Slovenia—SI
- South Africa—ZA
- South Korea—KR
- Spain—ES
- Sweden—SE
- Switzerland—CH
- Taiwan—TW
- Thailand—TH
- United Arab Emirates—AE
- United Kingdom—GB
- United States—US

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

default-cluster

Syntax default-cluster;

Hierarchy Level [edit wlan cluster *ID*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description (Optional) Specify this as the default cluster for the interface.

Options *ID*—ID of the access point cluster. Enter a string of up to 64 characters.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

disable-dot11d

Syntax disable-dot11d;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description (Optional) For radios operating in the 2.4 GHz band, suppress the country code setting from being broadcast in beacons.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

dot1x

Syntax

```
dot1x {
   radius-server ip-address;
   radius-key secret-key;
   broadcast-key-refresh-rate minutes;
   session-key-refresh-rate minutes;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure 802.1x (also known as dynamic WEP) for generation and distribution of keys.

Options

radius-server—IP address of the RADIUS server. The default IP address is **192.168.1.10**.

radius-key—Key used by the RADIUS server, in the form of a string of up to 64 bytes. The default key is **secret**.

broadcast-key-refresh-rate—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

session-key-refresh-rate—Interval, in minutes, between session key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

dot1x-supplicant

Syntax

```
dot1x-supplicant {
   username username;
   password password;
}
```

Hierarchy Level [edit wlan access-point *name* external]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure 802.1x supplicant information for access point.

Options **dot1x-supplicant**—Configure username and password for 802.1x supplicant authentication:

- **username**—User identification. Specify a string of up to 64 bytes. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **password**—Password. Specify a string of up to 64 bytes. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, numeric digits, and special symbols such as @ and #.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

dtim-period

Syntax dtim-period *beacons*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure interval, in number of radio beacons transmitted, at which clients in power-save mode check for buffered data from the radio.

Options **dtim-period**—Specify a value from 1 to 255. The default is 2 beacons.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

ethernet

Syntax

```
ethernet {
   management-vlan vlan-id;
   name-server {
      ip-address1 ip-address2;
   }
   static {
      address ip-address/mask;
      default-gateway ip-address;
   }
   untagged-vlan vlan-id;
}
```

Hierarchy Level [edit wlan access-point *name* external system ports]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure Ethernet port on the access point.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

external

Syntax

```
external {
  dot1x-supplicant {
    username username;
    password password;
  }
  system {
    console {
      baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
    }
    ntp-server name;
    ports {
      ethernet {
        management-vlan vlan-id;
        name-server {
          ip-address1 ip-address2;
        }
        static {
          address ip-address/mask;
          default-gateway ip-address;
        }
        untagged-vlan vlan-id;
      }
    }
  }
}
```

Hierarchy Level [edit wlan access-point *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure access point network options.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

fixed-multicast-rate

Syntax fixed-multicast-rate (auto | *rate*);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure multicast/broadcast transmission rate.

Options **fixed-multicast-rate**—Specify either a specified speed or **auto**. The default is **auto**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

fragmentation-threshold

Syntax fragmentation-threshold *size*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure size at which a frame is divided into multiple 802.11 frames.

Options **fragmentation-threshold**—Specify an even number from **256** to **2346**. The default is **2346**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

http-redirect

Syntax

```
http-redirect {
   redirect-url url;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure HTTP redirection for a virtual access point.

Options **redirect-url** *url*—Redirect the user's first HTTP access to a specified webpage. This option is commonly used for Wi-Fi hotspots.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

 Copyright © 2011, Juniper Networks, Inc.

interfaces

Syntax

```
interfaces {
   interface name;
}
```

Hierarchy Level [edit wlan cluster *ID*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the interfaces that are part of this cluster.

Options ***ID***—ID of the access point cluster. Enter a string of up to 64 characters.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

logging-options

Syntax

```
logging-options {
   enable-persistent;
   enable-remote;
   log-server-address <ip-address>;
   log-server-port <port-number>;
}
```

Hierarchy Level
[edit wlan access-point *name*]
[edit wlan cluster *name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure access point logging options.

Options

- ***enable-persistent***—Specifies that an Access Point stores all persistent log events to internal flash memory and remote server or services gateway periodically fetches these system log messages files from all the Access Points.
- ***enable-persistent***—Specifies that system log messages files are not stored on internal flash and will be sent to remote log server directly.
- ***log-server-address***—Specifies the IP address of the remote log server.
- ***log-server-port***—Specifies the port of the remote log server.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

mac-authentication-type

Syntax mac-authentication-type (disabled | local | radius);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable or disable client authentication using the client's MAC address.

Options **disable**—No MAC authentication is performed. This is the default.

local—The client's MAC address is looked up on a list of configured MAC addresses. Use the **station-mac-filter** configuration statement to configure the MAC addresses that are allowed or denied access.

radius—The client's MAC address is authenticated with a RADIUS server.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

management-vlan

Syntax management-vlan *vlan-id*;

Hierarchy Level [edit wlan access-point *name* external system ports ethernet]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure VLAN for management traffic for access point.

Options **management-vlan**—Identifier for VLAN for management traffic. Specify a value from 1 to 4094. The default is 1.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

maximum-stations

Syntax maximum-stations *number*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure maximum number of associations the radio can support.

Options **maximum-stations**—Specify a value from 0 to 200. The default is 200.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

maximum-burst

Syntax maximum-burst *microseconds*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service access-point-queues *queue*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure maximum length, in microseconds, allowed for packet bursts on the wireless network. (A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.)

Options **maximum-burst**—Specify a value from 0 to 999900. The defaults are 1500 microseconds for **voice-queue**, 3000 microseconds for **video-queue**, and 0 microseconds for **best-effort-queue** and **background-queue**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

maximum-contention-window

Syntax maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure upper limit, in slots, for the doubling of the random back-off time; doubling of the random back-off time continues until either the data frame is sent or this value is reached.

Options **maximum-contention-window**—Specify one of the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The defaults are 7 slots for **voice-queue**, 15 slots for **video-queue**, 63 slots for **best-effort-queue**, and 1023 slots for **background-queue**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

minimum-contention-window

Syntax minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure upper limit, in slots, of a range from which the initial random back-off wait time is determined. The first random number generated will be a number between 0 and the value specified. If the first random back-off wait time expires before the data frame is sent, a retry counter is incremented and the random back-off value is doubled. Doubling continues until the size of the random back-off values reaches the value defined in **maximum-contention-window**.

Options **minimum-contention-window**—Specify one of the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The defaults are 3 slots for **voice-queue**, 7 slots for **video-queue**, and 15 slots for **best-effort-queue** and **background-queue**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

mode

Syntax mode (2.4GHz | 5GHz | a | an | bg | bgn);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set Physical Layer (PHY) standard mode of the radio.

Options **mode**—Default for radio 1 is 802.11b/g/n; default for radio 2 is 802.11a/n. Select one of the following values:

- **2.4GHz**—2.4 GHz 802.11n
- **5GHz**—5 GHz 802.11n
- **a**—802.11a
- **an**—802.11a/n
- **bg**—802.11b/g
- **bgn**—802.11b/g/n

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

name

Syntax name;

Hierarchy Level [edit wlan cluster *ID*]

Release Information Statement introduced in Release 10.1 of Junos OS.

Description Specify the name of the cluster.

Options ***ID***—ID of the access point cluster. Enter a string of up to 64 characters.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

name-server

Syntax

```
name-server {
   ip-address ;
}
```

Hierarchy Level [edit wlan access-point *name* external system ports ethernet]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure DNS server for access point.

Options **name-server**— IP address of Domain Name System (DNS) server.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

no-acknowledgement

Syntax no-acknowledgement;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Suppress sending of acknowledgments (acks) by the access point when a frame is correctly received, per IEEE 802.11e standard.

NOTE: This configuration statement has no effect if Wi-Fi Multimedia (WMM) is disabled.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

no-auto-power-save

Syntax no-auto-power-save;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Disable Automatic Power Save Delivery (APSD), per IEEE 802.11e standard. APSD is recommended if VoIP phones access the network through the access point.

NOTE: Disabling or enabling APSD has no effect if Wi-Fi Multimedia (WMM) is disabled.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

no-broadcast-ssid

Syntax no-broadcast-ssid;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Disable access point responses to client broadcast probes.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

no-short-guard-interval-supported

Syntax no-short-guard-interval-supported;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Disable 802.11n Short Inter-Symbol Guard Interval.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

no-wifi-multimedia

Syntax no-wifi-multimedia;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Disable Wi-Fi MultiMedia (WMM). Disabling WMM deactivates QoS control of parameters on traffic from the client to the access point. With WMM disabled, you can still set some parameters on traffic from the access point to the client.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

ntp-server

Syntax ntp-server *name*;

Hierarchy Level [edit wlan access-point *name* external system]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure Network Time Protocol (NTP) server for access point.

Options **ntp-server**—NTP server name.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

protection

Syntax protection (auto | off);

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable or disable protection mechanisms to prevent interference with legacy client and access points from 802.11n or 802.11g transmissions.

Options **protection** —Specify **auto** or **off**. The default is **auto**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

quality-of-service

Syntax

```
quality-of-service {
  access-point-queues {
    background-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    best-effort-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    video-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    voice-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
  }
  no-acknowledgement;
  no-auto-power-save;
  no-wifi-multimedia;
  station-queues {
    background-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    best-effort-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    video-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    voice-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
```

```
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure quality of service (QoS) for the radio.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

radio

Syntax

```
radio ( 1 | 2 ){
  quality-of-service {
    access-point-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      video-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      voice-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      voice-queue {
        arbitration-inter-frame-space slots;
```

```
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
radio-options {
    beacon-interval ms;
    broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
    }
    channel {
        number ( auto | channel-number );
        bandwidth (20 | 40 );
        primary ( lower | upper );
    }
    disable-dot11d;
    dtim-period beacons;
    fixed-multicast-rate ( auto | rate );
    fragmentation-threshold size;
    maximum-stations number;
    mode (2.4GHz | 5GHz | a | an | bg | bgn);
    no-short-guard-interval-supported;
    protection ( auto | off );
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
        supported-rates rate1 rate2 ... rate-n;
        supported-basic-rates rate1 rate2 ... rate-n;
    }
}
virtual-access-point id {
    description description;
    http-redirect {
        redirect-url url;
    }
    no-broadcast-ssid;
    security {
        dot1x {
            radius-server ip-address;
            radius-key secret-key;
            broadcast-key-refresh-rate minutes;
            session-key-refresh-rate minutes;
        }
        mac-authentication-type ( disabled | local | radius );
        none;
        static-wep {
            authentication-type (open | shared | both);
            key-length (64bits | 128bits);
            key-type ( ascii | hex );
            transfer-key-index id;
            wep-key-1 key-1;
            wep-key-2 key-2;
```

 Copyright © 2011, Juniper Networks, Inc.

```
            wep-key-3 key-3;
            wep-key-4 key-4;
          }
          wpa-enterprise {
            cipher-suites (tkip | ccmp | both);
            pre-authenticate;
            radius {
              radius-server ip-address;
              radius-key secret-key;
              broadcast-key-refresh-rate minutes;
              session-key-refresh-rate minutes;
            }
            wpa-version (v1 | v2 | both);
          }
          wpa-personal {
            broadcast-key-refresh-rate minutes;
            cipher-suites (tkip | ccmp | both);
            key key;
            wpa-version (v1 | v2 | both);
          }
        }
        ssid ssid;
        vlan vlan-id;
      }
    }
```

Hierarchy Level [edit wlan access-point *name*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure radio 1 or radio 2 on the access point.

Options The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

radio-off

Syntax radio-off;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Set operational state of radio to off.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

radio-options

Syntax

```
radio-options {
  beacon-interval ms;
  broadcast-multicast-rate-limit {
    rate-limit packets-per-second;
    rate-limit-bursts packets-per-second;
  }
  channel {
    number ( auto | channel-number );
    bandwidth (20 | 40 );
    primary ( lower | upper );
  }
  disable-dot11d;
  dtim-period beacons;
  fixed-multicast-rate ( auto | rate );
  fragmentation-threshold size;
  maximum-stations number;
  mode (2.4GHz | 5GHz | a | an | bg | bgn);
  no-short-guard-interval-supported;
  protection ( auto | off );
  radio-off;
  rts-threshold size;
  space-time-block-coding;
  transmit-power percent;
  transmit-rate-sets {
    supported-rates rate1 rate2 ... rate-n;
    supported-basic-rates rate1 rate2 ... rate-n;
  }
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure access point radio.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

rts-threshold

Syntax rts-threshold *size*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure size of a request to send (RTS) transmission packet.

Options **rts-threshold**—Specify a value from 0 to 2347. The default is 2347.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

security

Syntax

```
security {
  dot1x {
    radius-server ip-address;
    radius-key secret-key;
    broadcast-key-refresh-rate minutes;
    session-key-refresh-rate minutes;
  }
  mac-authentication-type ( disabled | local | radius );
  none;
  static-wep {
    authentication-type (open | shared | both);
    key-length (64bits | 128bits);
    key-type ( ascii | hex );
    transfer-key-index id;
    wep-key-1 key-1;
    wep-key-2 key-2;
    wep-key-3 key-3;
    wep-key-4 key-4;
  }
  wpa-enterprise {
    cipher-suites (tkip | ccmp | both);
    pre-authenticate;
    radius {
      radius-server ip-address;
      radius-key secret-key;
      broadcast-key-refresh-rate minutes;
      session-key-refresh-rate minutes;
    }
    wpa-version (v1 | v2 | both);
  }
  wpa-personal {
    broadcast-key-refresh-rate minutes;
    cipher-suites (tkip | ccmp | both);
    key key;
    wpa-version (v1 | v2 | both);
  }
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure security for the virtual access point.

Options The remaining statements are explained separately.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

space-time-block-coding

Syntax space-time-block-coding;

Hierarchy Level [edit wlan access-point *name* radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Enable 802.11n Space Time Block Coding (STBC).

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

ssid

Syntax ssid *ssid*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure Service Set Identifier (SSID) broadcast by the access point.

Options **ssid *id***—String of up to 32 characters.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

static

Syntax

```
static {
   address ip-address/mask;
   default-gateway ip-address;
}
```

Hierarchy Level [edit wlan access-point *name* external system ports ethernet]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure static IP address information for the access point.

Options **address**—IP address and netmask for the access point.

default-gateway—IP address of the default gateway.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

static-wep

Syntax

```
static-wep {
   authentication-type (open | shared | both);
   key-length (64bits | 128bits);
   key-type ( ascii | hex );
   transfer-key-index id;
   wep-key-1 key-1;
   wep-key-2 key-2;
   wep-key-3 key-3;
   wep-key-4 key-4;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure a preshared Wired Equivalent Privacy (WEP) key.

Options

authentication-type—Specify **open** to allow any client to associate with the access point; clients must have the correct WEP key to transmit and received encrypted data. Specify **shared** to permit only clients with the correct WEP key to associate with the access point. Specify **both** to allow both open and shared authentication.

static wep—Configure a preshared Wired Equivalent Privacy (WEP) key.

key-length—Length, in bits, of WEP key. Specify **64bits** for 64 bits or **128bits** for 128 bits. The default is 64 bits.

key-type—Format of the WEP key. Specify either **ascii** for ASCII format or **hex** for hexadecimal format. The default is ASCII.

transfer-key-index—Allow configuration of up to four preshared keys. Specify a value from 1 to 4.

wep-key-1 through **wep-key-4**—Preshared key string that corresponds to the **transfer-key-index** value.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

station-mac-filter

Syntax

```
station-mac-filter {
   ( allow-list | deny-list );
   mac-address addr1 addr2 ... addrn;
}
```

Hierarchy Level [edit wlan access-point *name* access-point-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure list of client MAC addresses for local authentication.

Options

allow-list—List of allowed MAC addresses.

deny-list—List of denied MAC addresses.

mac-address—Client MAC address.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

station-queues

Syntax

```
station-queues {
  background-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  best-effort-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  video-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  voice-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
}
```

Hierarchy Level

[edit wlan access-point *name* radio (1 | 2) quality-of-service]

Release Information

Statement introduced in Release 10.0 of Junos OS.

Description

Configure enhanced distributed channel access (EDCA) parameters for upstream traffic from the client to the access point.

Options

Options can be configured for the following queues:

- **voice-queue**—Highest priority queue with minimum delay.
- **video-queue**—High priority queue with minimum delay.
- **best-effort-queue**—Medium priority queue with medium throughput and delay.
- **background-queue**—Lowest priority queue with high throughput.

The remaining statements are explained separately.

Required Privilege Level

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

syslog-options

Syntax

```
syslog-options {
   log-size <number>;
   period <number>;
}
```

Hierarchy Level [edit wlan access-point *name*]

Release Information Statement introduced in Release 11.1 of Junos OS.

Description Configure access point logging options.

Options

- ***log-size***—Maximum size of each system log file that can be stored on an access point. Range (4 to 1024 kilobytes)
- ***period***—Specifies the interval, in seconds, between retrieving and storing syslog messages on the SRX Series device. Range (60 through 86,400 seconds)

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

transmit-opportunity-limit

Syntax transmit-opportunity-limit *ms*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service station-queues *queue*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure interval, in milliseconds, when a WMM client can initiate transmissions onto the wireless network.

Options **transmit-opportunity-limit**—Specify a value from 0 through 65,535. The defaults are 47 ms for **voice-queue**, 94 ms for **video-queue**, and 0 ms for **best-effort-queue** and **background-queue**.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

transmit-power

Syntax transmit-power *percent*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure percent of radio transmit power.

Options Specify a value from 0 to 100. The default is 100.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

transmit-rate-sets

Syntax

```
transmit-rate-sets {
   supported-rates rate1 rate2 ... rate-n;
   supported-basic-rates rate1 rate2 ... rate-n;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) radio-options]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Specify the transmission rates supported by and advertised by the radio. Valid rates are determined by the radio's **mode** setting.

Options

supported-rates—Transmission rates supported by the radio.

supported-basic-rates—Transmission rates advertised by the radio.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

untagged-vlan

Syntax untagged-vlan *vlan-id*;

Hierarchy Level [edit wlan access-point *name* external system ports ethernet]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure VLAN for untagged traffic for the access point.

Options **untagged-vlan**—Identifier for VLAN to which untagged traffic is assigned. Specify a value from 1 to 4094. The default is 1.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

video-queue

Syntax For access-point-queues:

```
video-queue {
   arbitration-inter-frame-space slots;
   maximum-burst microseconds;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
video-queue {
   arbitration-inter-frame-space slots;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   transmit-opportunity-limit ms;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure high priority queue with minimum delay.

Options The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

virtual-access-point

Syntax

```
virtual-access-point id {
  description description;
  http-redirect {
    redirect-url url;
  }
  no-broadcast-ssid;
  security {
    dot1x {
      radius-server ip-address;
      radius-key secret-key;
      broadcast-key-refresh-rate minutes;
      session-key-refresh-rate minutes;
    }
    mac-authentication-type ( disabled | local | radius );
    none;
    static-wep {
      authentication-type (open | shared | both);
      key-length (64bits | 128bits);
      key-type ( ascii | hex );
      transfer-key-index id;
      wep-key-1 key-1;
      wep-key-2 key-2;
      wep-key-3 key-3;
      wep-key-4 key-4;
    }
    wpa-enterprise {
      cipher-suites (tkip | ccmp | both);
      pre-authenticate;
      radius {
        radius-server ip-address;
        radius-key secret-key;
        broadcast-key-refresh-rate minutes;
        session-key-refresh-rate minutes;
      }
      wpa-version (v1 | v2 | both);
    }
    wpa-personal {
      broadcast-key-refresh-rate minutes;
      cipher-suites (tkip | ccmp | both);
      key key;
      wpa-version (v1 | v2 | both);
    }
  }
  ssid ssid;
  vlan vlan-id;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure virtual access point for an access point radio.

Copyright © 2011, Juniper Networks, Inc.

Options **virtual-access-point** ***id***—Virtual access point identifier. Specify an identifier from 0 through 15.

NOTE: VAP 0 is the physical radio interface. VAP 0 is assigned to the BSSID of the physical radio interface.

NOTE: VAP 0 is always enabled. To disable VAP 0, the radio itself must be disabled.

description—Description of the virtual access point.

The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

vlan

Syntax vlan *vlan-id*;

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure the VLAN associated with the virtual access point.

Options **vlan** ***vlan-id***—Specify a VLAN ID from 1 to 4094. The default is 1.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

voice-queue

Syntax For access-point-queues:

```
voice-queue {
   arbitration-inter-frame-space slots;
   maximum-burst microseconds;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
voice-queue {
   arbitration-inter-frame-space slots;
   maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
   transmit-opportunity-limit ms;
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure highest priority queue with minimum delay.

Options The remaining statements are explained separately.

Required Privilege Level wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

wpa-enterprise

Syntax

```
wpa-enterprise {
   cipher-suites (tkip | ccmp | both);
   pre-authenticate;
   radius {
      radius-server ip-address;
      radius-key secret-key;
      broadcast-key-refresh-rate minutes;
      session-key-refresh-rate minutes;
   }
   wpa-version (v1 | v2 | both);
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure RADIUS authentication with TKIP and/or CCMP encryption.

Options

cipher-suites—Encryption type. Specify **tkip**, **ccmp**, or **both**.

pre-authenticate—Enable 802.11i pre-authentication.

radius-server—IP address of the RADIUS server. The default IP address is **192.168.1.10**.

radius-key—Key used by the RADIUS server, in the form of a string of up to 64 bytes. The default key is **secret**.

broadcast-key-refresh-rate—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

session-key-refresh-rate—Interval, in minutes between session key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

wpa-version—WPA version. Specify **v1**, **v2**, or **both**.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

wpa-personal

Syntax

```
wpa-personal {
   broadcast-key-refresh-rate minutes;
   cipher-suites ( tkip | ccmp | both );
   key key;
   wpa-version (v1 | v2 | both);
}
```

Hierarchy Level [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

Release Information Statement introduced in Release 10.0 of Junos OS.

Description Configure preshared key with Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP) and/or Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption.

Options

broadcast-key-refresh-rate—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

cipher-suites—Encryption type. Specify **tkip**, **ccmp**, or **both**.

key—Preshared key.

wpa-version—WPA version. Specify **v1**, **v2**, or **both**.

Required Privilege Level
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

Copyright © 2011, Juniper Networks, Inc.

PART 2

Operational Commands

- Clear Commands on page 1001
- Request Commands on page 1091
- Restart Commands on page 1133
- Show Commands on page 1137

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 24

Clear Commands

This section contains the following topics:

- Clear Commands Overview on page 1001

Clear Commands Overview

Use the **clear** configuration commands to clear information about the following features and protocols: Address Resolution Protocol (ARP), auto-configuration, Bidirectional Forwarding Detection (BFD), Border Gateway Protocol (BGP), chassis, 802.1X, End System-to-Intermediate System (ES-IS), Ethernet switching, firewall counters, Generic VLAN Registration Protocol (gvrp), port-forwarding helper, Internet Group Management Protocol (IGMP), IGMP snooping, interfaces, IP version 6 (IPv6), Integrated Services Digital Network (ISDN), Intermediate System-to-Intermediate System (IS-IS), Link Aggregation Control Protocol (LACP), Label Distribution Protocol (LDP), Link Layer Discovery Protocol (LLDP), log file contents, Multicast Listener Discovery, mobile IP, Multiprotocol Label Switching (MPLS), Multicast Source Discovery Protocol (MSDP), multicast, network access, Open Shortest Path First (OSPF), Open Shortest Path First version 3 (OSPFv3), passive monitoring statistics, Packet Forwarding Engine (PFE), Pragmatic Generalized Multicast (PGM), Protocol Independent Multicast (PIM), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Routing Information Protocol (RIP), Routing Information Protocol for IPv6 (RIPng), Resource Reservation Protocol (RSVP), security, services, Simple Network Management Protocol (SNMP), Spanning Tree Protocol, system, Virtual Private LAN Service (VPLS), and Virtual Router Redundancy Protocol.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*.
- *Junos OS System Basics and Services Command Reference*.

clear chassis cluster control-plane statistics

Syntax **clear chassis cluster control-plane statistics**

Release Information Command introduced in Release 9.3 of Junos OS.

Description Clear the control plane statistics of a chassis cluster.

Required Privilege Level clear

Related Documentation

- **show chassis cluster control-plane statistics on page 1143**

List of Sample Output **clear chassis cluster control-plane statistics on page 1002**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear chassis cluster control-plane statistics

```
user@host> clear chassis cluster control-plane statistics
Cleared control-plane statistics
```


Copyright © 2011, Juniper Networks, Inc.

clear chassis cluster data-plane statistics

Syntax **clear chassis cluster data-plane statistics**

Release Information Command introduced in Release 9.3 of Junos OS.

Description Clear the data plane statistics of a chassis cluster.

Required Privilege Level clear

Related Documentation

- **show chassis cluster data-plane statistics on page 1146**

List of Sample Output **clear chassis cluster data-plane statistics on page 1003**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear chassis cluster data-plane statistics

```
user@host> clear chassis cluster data-plane statistics
Cleared data-plane statistics
```

clear chassis cluster failover-count

Syntax **clear chassis cluster failover-count**

Release Information Command introduced in Release 9.3 of Junos OS.

Description Clear the failover count of all redundancy-groups.

Required Privilege Level clear

Related Documentation

- **request chassis cluster failover node on page 1095**
- **request chassis cluster failover reset on page 1096**
- **show chassis cluster status on page 1157**

List of Sample Output

show chassis cluster status on page 1004
clear chassis cluster failover-count on page 1004
show chassis cluster status on page 1004

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output The following example displays the redundancy groups before and after the failover-counts are cleared.

show chassis cluster status

```
user@host> show chassis cluster status

Cluster ID: 3
Node name         Priority     Status     Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
   node0            200        secondary   no        no
   node1            100        primary     no        no

Redundancy group: 1 , Failover count: 2
   node0            100        primary     no        no
   node1            10         secondary   no        no
```

clear chassis cluster failover-count

```
user@host> clear chassis cluster failover-count
Cleared failover-count for all redundancy-groups
```

show chassis cluster status

```
user@host> show chassis cluster status

Cluster ID: 3
Node name        Priority   Status     Preempt  Manual failover

Redundancy group: 0 , Failover count: 0
  node0           200       secondary    no       no
  node1           100       primary      no       no

Redundancy group: 1 , Failover count: 0
  node0           100       primary      no       no
```

 Copyright © 2011, Juniper Networks, Inc.

```
node1            10        secondary    no       no
```

clear chassis cluster ip-monitoring failure-count

Syntax clear chassis cluster ip-monitoring failure-count

Release Information Command introduced in Release 10.1 of Junos OS.

Description Clear the failure count for all IP addresses.

Required Privilege Level clear

Related Documentation

- **clear chassis cluster failover-count on page 1004**

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

user@host> **clear chassis cluster ip-monitoring failure-count**

```
node0:
--------------------------------------------------------------------------
Cleared failure count for all IPs

node1:
--------------------------------------------------------------------------
Cleared failure count for all IPs
```


Copyright © 2011, Juniper Networks, Inc.

clear chassis cluster ip-monitoring failure-count ip-address

Syntax clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1

Release Information Command introduced in Release 10.1 of Junos OS.

Description Clear the failure count for a specified IP address.

NOTE: Entering an IP address at the end of this command is optional. If you do not specify an IP address, the failure count for all monitored IP addresses is cleared.

Required Privilege Level clear

Related Documentation

- **clear chassis cluster failover-count on page 1004**

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

user@host> **clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1**

```
node0:
--------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1

node1:
--------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1
```

clear chassis cluster statistics

Syntax **clear chassis cluster statistics**

Release Information Command introduced in Release 9.3 of Junos OS.

Description Clear the control plane and data plane statistics of a chassis cluster.

Required Privilege Level clear

Related Documentation

- **show chassis cluster statistics on page 1153**

List of Sample Output **clear chassis cluster statistics on page 1008**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear chassis cluster statistics

```
user@host> clear chassis cluster statistics
Cleared control-plane statistics
Cleared data-plane statistics
```


Copyright © 2011, Juniper Networks, Inc.

clear dhcpv6 server binding

Syntax

clear dhcpv6 server binding
<all | *client-id* | *ip-address* | *session-id*>
<interface *interface-name*>
<routing-instance *routing-instance-name*>

Release Information

Command introduced in Junos Release 10.4.

Description

Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

Options

all—(Optional) Clear the binding state for all DHCPv6 clients.

client-id—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).

ip-address—(Optional) Clear the binding state for the DHCPv6 client with the specified address.

session-id—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.

interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level

clear

Related Documentation

- **show dhcpv6 server binding on page 1171**

clear dhcpv6 server statistics

Syntax clear dhcpv6 server statistics

Release Information Command introduced in Junos Release 10.4.

Description Clear all DHCPv6 local server statistics.

Options routing-instance *routing-instance-name*—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- **show dhcpv6 server statistics on page 1175**

 Copyright © 2011, Juniper Networks, Inc.

clear esis adjacency

Syntax

clear esis adjacency
<instance *instance-name*>
<interface *interface-name*)>
<*neighbor*>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Clear End System-to-Intermediate System (ES-IS) adjacencies.

Options

none—Clear all ES-IS adjacencies.

instance *instance-name*—(Optional) Clear adjacencies for the specified routing instance only.

interface *interface-name*—(Optional) Clear adjacencies for the specified interface only.

neighbor—(Optional) Clear adjacencies for the specified neighbor only.

Required Privilege Level

clear

Related Documentation

- **show esis adjacency on page 1177**

List of Sample Output

clear esis adjacency on page 1011

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear esis adjacency

`user@host>` **clear esis adjacency**

clear esis statistics

Syntax

clear esis statistics
<instance *instance-name*>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Clear End System-to-Intermediate System (ES-IS) packet statistics.

Options

none—Clear ES-IS packet statistics for all routing instances.

instance *instance-name*—(Optional) Clear ES-IS packet statistics for the specified routing instance only.

Required Privilege Level

clear

Related Documentation

- **show esis statistics on page 1181**

List of Sample Output

clear esis statistics on page 1012

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear esis statistics

`user@host>` **clear esis statistics**

Copyright © 2011, Juniper Networks, Inc.

clear gtp tunnels

Syntax **clear security gprs gtp tunnel <all | *identifier*>**

Release Information Command introduced in Release 10.0 of Junos OS.

Description Clear all or specified GTP tunnels on the device.

Options

- *identifier*—Clear a single tunnel by entering the tunnel ID. To view current tunnel IDs, type **show security gprs gtp tunnels**
- all—Clear all existing tunnels

Required Privilege Level clear

Copyright © 2011, Juniper Networks, Inc.

clear interfaces statistics swfabx

Syntax clear interfaces statistics <swfab0 | swfab1>

Release Information Command introduced in Release 11.1 of Junos OS.

Description Clears interface statistics for the specified swfab interface.

Required Privilege Level clear

Related Documentation

- **show interfaces swfabx on page 1216**

List of Sample Output **clear interfaces statistics <swfab0 | swfab1> on page 1014**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear interfaces statistics <swfab0 | swfab1>

```
user@host> clear interfaces statistics <swfab0 | swfab1>
```


Copyright © 2011, Juniper Networks, Inc.

clear lacp statistics interfaces

Syntax **clear lacp statistics interfaces** <*interface-name*>

Release Information Command modified in Release 10.2 of Junos OS.

Description Clear the LACP statistics. If you do not specify an interface name, LACP statistics for all interfaces are cleared.

Options *interface-name*—(Optional) Name of an interface.

Required Privilege Level clear

Related Documentation

- **show lacp statistics interfaces on page 1221**

Output Fields This command produces no output.

clear network-access requests pending

Syntax

clear network-access requests pending
<index *index-number* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Clear or cancel all pending authentication requests.

Options

none—Clear all network access requests pending.

index *index-number* —Clear the specified authentication request. To display index numbers, use the **show network-access requests pending** command.

Required Privilege Level

clear

Related Documentation

- **show network-access requests pending on page 1230**

List of Sample Output

clear network-access requests pending on page 1016

Output Fields

This command produces no output.

Sample Output

The following example displays the network access requests that are pending, clears the requests, and displays the results of the clear operation:

clear network-access requests pending

```
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                  Status
1     Sun                   Processing
2     Sam                   Processed

user@host> clear network-access requests pending
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                  Status
1     Sun                   Cancelled by Admin
2     Sam                   Cancelled by Admin
```


Copyright © 2011, Juniper Networks, Inc.

clear network-access requests statistics

Syntax clear network-access requests statistics

Release Information Command introduced in Release 8.5 of Junos OS.

Description Clear general authentication statistics for the configured authentication type.

Required Privilege Level clear

Related Documentation

- **authentication-order on page 12**
- **show network-access requests statistics on page 1232**

List of Sample Output **clear network-access requests statistics on page 1017**

Output Fields This command produces no output.

clear network-access requests statistics

```
user@host> clear network-access requests statistics
```

clear network-access securid-node-secret-file

Syntax clear network-access securid-node-secret-file

Release Information Command introduced in Release 9.1 of Junos OS.

Description Delete the node secret file for the SecurID authentication type.

Required Privilege Level clear

Related Documentation

- configuration-file on page 17
- securid-server on page 44
- show network-access securid-node-secret-file on page 1233

List of Sample Output clear network-access securid-node-secret-file on page 1018

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear network-access securid-node-secret-file

```
user@host> clear network-access securid-node-secret-file
```


Copyright © 2011, Juniper Networks, Inc.

clear security alg h323 counters

Syntax

clear security alg h323 counters
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear information about H.323 Application Layer Gateway (ALG) counters.

Options

none—Clear H.323 ALG counters.

node—(Optional) For chassis cluster configurations, clear H.323 counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **h323 on page 483**
- **show security alg h323 counters on page 1241**

List of Sample Output

clear security alg h323 counters on page 1019

Output Fields

This command produces no output.

clear security alg h323 counters

```
user@host> clear security alg h323 counters
```

clear security alg ike-esp-nat

Syntax clear security alg ike-esp-nat

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear state information about Application Layer Gateway (ALG) for IKE and ESP.

Required Privilege Level clear

Related Documentation

- **show security alg ike-esp-nat summary on page 1243**

List of Sample Output **clear security alg ike-esp-nat on page 1020**

Output Fields This command produces no output.

clear security alg ike-esp-nat

```
user@host> clear security alg ike-esp-nat
10 active IKE-ESP alg state cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security alg mgcp calls

Syntax

clear security alg mgcp calls
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) calls.

Options

none—Clear all MGCP ALG calls.

node—(Optional) For chassis cluster configurations, clear MGCP calls on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **mgcp on page 575**
- **show security alg mgcp calls on page 1244**

List of Sample Output

clear security alg mgcp calls on page 1021

Output Fields

This command produces no output.

clear security alg mgcp calls

```
user@host> clear security alg mgcp calls
```

clear security alg mgcp counters

Syntax

clear security alg mgcp counters
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) counter information.

Options

none—Clear all MGCP ALG counters.

node—(Optional) For chassis cluster configurations, clear MGCP counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **mgcp on page 575**
- **show security alg mgcp counters on page 1246**

List of Sample Output

clear security alg mgcp counters on page 1022

Output Fields

This command produces no output.

clear security alg mgcp counters

```
user@host> clear security alg mgcp counters
```


Copyright © 2011, Juniper Networks, Inc.

clear security alg sccp calls

Syntax

clear security alg sccp calls
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Skinny Client Protocol (SCCP) Application Layer Gateway (ALG) call information.

Options

none—Clear all SCCP ALG calls.

node—(Optional) For chassis cluster configurations, clear SCCP calls on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **sccp on page 696**
- **show security alg sccp calls on page 1252**

List of Sample Output

clear security alg sccp calls on page 1023

Output Fields

This command produces no output.

clear security alg sccp calls

```
user@host> clear security alg sccp calls
```

clear security alg sccp counters

Syntax

clear security alg sccp counters
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

Options

none—Clear all SCCP ALG counters.

node—(Optional) For chassis cluster configurations, clear SCCP counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **sccp on page 696**
- **show security alg sccp counters on page 1254**

List of Sample Output

clear security alg sccp counters on page 1024

Output Fields

This command produces no output.

clear security alg sccp counters

```
user@host> clear security alg sccp counters
```


Copyright © 2011, Juniper Networks, Inc.

clear security alg sip calls

Syntax

clear security alg sip calls
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) call information.

Options

none—Clear all SIP ALG calls.

node—(Optional) For chassis cluster configuration, clear SIP calls on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **sip on page 724**
- **show security alg sip calls on page 1256**

List of Sample Output

clear security alg sip calls on page 1025

Output Fields

This command produces no output.

clear security alg sip calls

```
user@host> clear security alg sip calls
```

clear security alg sip counters

Syntax

clear security alg sip counters
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

Options

none—Clear all SIP ALG counters.

node—(Optional) For chassis cluster configurations, clear SIP counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **sip on page 724**
- **show security alg sip counters on page 1258**

List of Sample Output

clear security alg sip counters on page 1026

Output Fields

This command produces no output.

clear security alg sip counters

```
user@host> clear security alg sip counters
```


Copyright © 2011, Juniper Networks, Inc.

clear security application-firewall rule-set statistics

Syntax **clear security application-firewall rule-set statistics**

Release Information Command introduced in Release 11.1 of Junos OS.

Description Clear all the security application firewall rule set statistics information.

Required Privilege Level clear

Related Documentation **show security application-firewall rule-set on page 1267**

Output Fields This command produces no output.

clear security datapath-debug counters

Syntax clear security datapath-debug counters

Release Information Command introduced in Release 10.0 of Junos OS.

Description Clear all data path-debugging counters.

Required Privilege Level clear

Related Documentation

- **show security datapath-debug capture on page 1270**
- **show security datapath-debug counter on page 1271**

List of Sample Output **clear security datapath-debug counters on page 1028**

Output Fields This command produces no output.

clear security datapath-debug counters

```
user@host> clear security datapath-debug counters
```


Copyright © 2011, Juniper Networks, Inc.

clear security dynamic-vpn all

Syntax clear security dynamic-vpn all

Release Information Command introduced in Junos Release 10.4.

Description Clear all dynamic VPN user connections.

Required Privilege Level clear

Related Documentation

- **show security dynamic-vpn users on page 1278**
- **show security dynamic-vpn users terse on page 1279**

List of Sample Output **clear security dynamic-vpn all on page 1029**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security dynamic-vpn all

```
user@host> clear security dynamic-vpn all
2 user connection entries cleared
```

clear security dynamic-vpn user

Syntax clear security dynamic-vpn user *username* ike-id *id*

Release Information Command introduced in Junos Release 10.4.

Description Clear the dynamic VPN user connection for the specified username.

Required Privilege Level clear

Related Documentation

- **show security dynamic-vpn users on page 1278**
- **show security dynamic-vpn users terse on page 1279**

List of Sample Output **clear security dynamic-vpn user on page 1030**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security dynamic-vpn user

```
user@host> clear security dynamic-vpn user guang ike-id bob.juniper.net
Connection entry for user guang has been cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security firewall-authentication history

Syntax

clear security firewall-authentication history
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear all firewall authentication history information.

Options

node—(Optional) For chassis cluster configurations, clear all firewall authentication history on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **firewall-authentication (Security) on page 453**
- **show security firewall-authentication history on page 1280**

List of Sample Output

clear security firewall-authentication history on page 1031
clear security firewall-authentication history node 1 on page 1031

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication history

```
user@host> clear security firewall-authentication history
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication history node 1

```
user@host> clear security firewall-authentication history node 1
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication history address

Syntax

clear security firewall-authentication history address *address*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear firewall authentication history for this source IP address.

Options

address *address* —Source IP address for which to clear firewall authentication history.

none—Clear all firewall authentication history for this address.

node—(Optional) For chassis cluster configurations, clear firewall authentication history for this address on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **firewall-authentication (Security) on page 453**
- **show security firewall-authentication history address on page 1282**

List of Sample Output

clear security firewall-authentication history address 100.0.0.1 on page 1032
clear security firewall-authentication history address 100.0.0.1 node 1 on page 1032

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication history address 100.0.0.1

```
user@host> clear security firewall-authentication history address 100.0.0.1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication history address 100.0.0.1 node 1

```
user@host> clear security firewall-authentication history address 100.0.0.1 node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2011, Juniper Networks, Inc.

clear security firewall-authentication history identifier

Syntax

clear security firewall-authentication history identifier *identifier*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.

Description

Clear firewall authentication history information for the authentication with this identifier.

Options

identifier *identifier* —Identification number of the authentication for which to clear authentication history.

none—Clear all firewall authentication history information for the authentication with this identifier.

node—(Optional) For chassis cluster configurations, clear firewall authentication history on a specific node for the authentication with this identifier.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **firewall-authentication (Security) on page 453**
- **show security firewall-authentication history identifier on page 1285**

List of Sample Output

clear security firewall-authentication history identifier 2 on page 1033
clear security firewall-authentication history identifier 2 node 1 on page 1033

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication history identifier 2

```
user@host> clear security firewall-authentication history identifier 2
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication history identifier 2 node 1

```
user@host> clear security firewall-authentication history identifier 2 node 1
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication users

Syntax

clear security firewall-authentication users
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear firewall authentication tables for all users.

Options

node—(Optional) For chassis cluster configurations, clear firewall authentication details for all users on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security firewall-authentication users on page 1288**

List of Sample Output

clear security firewall-authentication users on page 1034
clear security firewall-authentication users node 1 on page 1034

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication users

```
user@host> clear security firewall-authentication users node 1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication users node 1

```
user@host> clear security firewall-authentication users node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2011, Juniper Networks, Inc.

clear security firewall-authentication users address

Syntax

clear security firewall-authentication users address *address*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear information about the users at the specified IP address that are currently authenticated.

Options

address *address* —IP address for which to clear user firewall authentication information.

none—Clear all the firewall authentication information for users at this IP address.

node—(Optional) For chassis cluster configurations, clear user firewall authentication entries on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security firewall-authentication users address on page 1290**

List of Sample Output

clear security firewall-authentication users address 100.0.0.1 on page 1035
clear security firewall-authentication users address 100.0.0.1 node 1 on page 1035

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication users address 100.0.0.1

```
user@host> clear security firewall-authentication users address 100.0.0.1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication users address 100.0.0.1 node 1

```
user@host> clear security firewall-authentication users address 100.0.0.1 node 1
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication users identifier

Syntax

clear security firewall-authentication users identifier *identifier*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear firewall authentication details about the user with this identification number.

Options

none—Identification number of the user for which to clear authentication details.

node—(Optional) For chassis cluster configurations, clear the firewall authentication details on a specific node (device) in the cluster for the user with this identification number.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security firewall-authentication users identifier on page 1292**

List of Sample Output

clear security firewall-authentication users identifier 2 on page 1036
clear security firewall-authentication users identifier 2 node 1 on page 1036

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security firewall-authentication users identifier 2

```
user@host> clear security firewall-authentication users identifier 2
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

clear security firewall-authentication users identifier 2 node 1

```
user@host> clear security firewall-authentication users identifier 2 node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2011, Juniper Networks, Inc.

clear security flow ip-action family

Syntax clear security flow ip-action family (inet | inet6)

Release Information Command introduced in Release 10.4 of Junos OS.

Description Clear currently active security sessions on the device.

Options inet—Clears IPv4 information.

inet6—Clears IPv6-NATPT information.

Required Privilege Level view

Related Documentation

- show security flow ip-action family on page 1341

Sample Output

```
user@host> clear security flow ip-action family inet6
0 ip-action entries cleared
```

clear security flow session all

Syntax

clear security flow session all
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear all currently active security sessions on the device.

Options

all—Clear information about all active sessions.

node—(Optional) For chassis cluster configurations, clear all security sessions on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session on page 1342**

List of Sample Output

clear security flow session all on page 1038
clear security flow session all node 0 on page 1038

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session all

```
user@host> clear security flow session all
node0:
--------------------------------------------------------------------------
1 active sessions cleared
node1:
-------- ------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session all node 0

```
user@host> clear security flow session all node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security flow session application

Syntax

clear security flow session application
application-name
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear currently active sessions for application types or application sets.

Options

application-name —Name of the specified application type or application set.

- **dns**—Domain Name System
- **ftp**—File Transfer Protocol
- **ignore**—Ignore application type
- **mgcp-ca**—Media Gateway Control Protocol with Call Agent
- **mgcp-ua**—MGCP with User Agent
- **ms-rpc**—Microsoft RPC
- **pptp**—Point-to-Point Tunneling Protocol
- **q931**—ISDN connection control protocol
- **ras**—RAS
- **realaudio**—RealAudio
- **rsh**—UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp**—Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **sqlnet-v2**—Oracle SQLNET
- **sun-rpc**—Sun Microsystems RPC
- **talk**—TALK program
- **tftp**—Trivial File Transfer Protocol

node—(Optional) For chassis cluster configurations, clear sessions for applications on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Copyright © 2011, Juniper Networks, Inc.

Required Privilege Level clear

Related Documentation

- **show security flow session application on page 1346**

List of Sample Output

clear security flow session application dns on page 1040
clear security flow session application dns node 0 on page 1040

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security flow session application dns

```
user@host> clear security flow session application dns
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session application dns node 0

```
user@host> clear security flow session application dns node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

 Copyright © 2011, Juniper Networks, Inc.

clear security flow session destination-port

Syntax

clear security flow session destination-port
destination-port-number
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear each session that uses the specified destination port

Options

destination-port-number —Number of the destination port.

node—(Optional) For chassis cluster configurations, clear security sessions on the port on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session destination-port on page 1354**

List of Sample Output

clear security flow session destination-port 1 on page 1041
clear security flow session destination-port 1 node 0 on page 1041

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session destination-port 1

```
user@host> clear security flow session destination-port 1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session destination-port 1 node 0

```
user@host> clear security flow session destination-port 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session destination-prefix

Syntax

clear security flow session destination-prefix
destination-IP-prefix
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS.
The **node** options added in Release 9.0 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.

Description

Clear sessions that match this destination IP prefix or address.

Options

destination-IP-prefix—Destination IP prefix or address.

node—(Optional) For chassis cluster configurations, clear sessions that match the IP prefix or address on a specific node (device) in the cluster.

- *node-id*—Identification number of the node. It can be 0 or 1.
- **all**—Clear all nodes.
- **local**—Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session destination-prefix on page 1358**

List of Sample Output

clear security flow session destination-prefix 100.0.0.1 on page 1042
clear security flow session destination-prefix 10::10 on page 1042
Clear security flow session destination-prefix 100.0.0.1 node 0 on page 1042

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session destination-prefix 100.0.0.1

```
clear security flow session destination-prefix 100.0.0.1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session destination-prefix 10::10

```
user@host> clear security flow session destination-prefix 10::10
1 active sessions cleared
```

Clear security flow session

```
user@host> clear security flow session destination-prefix 100.0.0.1 node 0
```


Copyright © 2011, Juniper Networks, Inc.

destination-prefix 100.0.0.1 node 0

```
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session family

Syntax clear security flow session family (inet | inet6)

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear sessions that match the specified protocol family.

Options **inet**—Clear IPv4 sessions.

inet6—Clear IPv6 sessions.

Required Privilege Level clear

Related Documentation

- **show security flow session family on page 1367**

List of Sample Output

clear security flow session family inet on page 1044
clear security flow session family inet6 on page 1044

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security flow session family inet

```
user@host> clear security flow session family inet
1 active sessions cleared
```

clear security flow session family inet6

```
user@host> clear security flow session family inet6
1 active sessions cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security flow session interface

Syntax

clear security flow session interface
interface-name
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear sessions that use the specified interface.

Options

interface-name —Name of a specific incoming or outgoing interface.

node—(Optional) For chassis cluster configurations, clear security sessions on the interface on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session interface on page 1374**

List of Sample Output

clear security flow session interface ge-0/0/0.0 on page 1045
clear security flow session interface ge/0/0.0 node 0 on page 1045

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session interface ge-0/0/0.0

```
user@host> clear security flow session interface ge-0/0/0.0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session interface ge/0/0.0 node 0

```
user@host> clear security flow session interface ge-0/0/0.0 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session protocol

Syntax

clear security flow session protocol *protocol-name* | *protocol-number*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear each session that uses the specified IP protocol.

Options

protocol-name — (Optional) Networking protocol name. The following text values are supported.

- **ah**—IP Security Authentication Header
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload
- **gre**—Generic routing encapsulation
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP over IP
- **ospf**—Open Shortest Path First
- **pim**—Protocol Independent Multicast
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

protocol-number —(Optional) Numeric protocol value. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

Range: 0 through 255

node—(Optional) For chassis cluster configurations, clear security on a specific node (device) in the cluster for the user with this identification number.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Copyright © 2011, Juniper Networks, Inc.

Related Documentation

- show security flow session protocol on page 1382

List of Sample Output

clear security flow session protocol pim on page 1047
clear security flow session protocol 0 on page 1047

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session protocol pim

```
user@host> clear security flow session protocol pim
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session protocol 0

```
user@host> clear security flow session protocol 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session resource-manager

Syntax

clear security flow session resource-manager
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear resource-manager sessions.

Options

node—(Optional) For chassis cluster configurations, clear the resource manager sessions on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session resource-manager on page 1387**

List of Sample Output

clear security flow session resource-manager on page 1048
clear security flow session resource-manager node 0 on page 1048

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session resource-manager

```
user@host> clear security flow session resource-manager
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session resource-manager node 0

```
user@host> clear security flow session resource-manager node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security flow session session-identifier

Syntax

clear security flow session session-identifier
session-identifier
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear the session with the specific identifier.

Options

session-identifier —Number from 1 through 4,294,967,295 that identifies the security session.

node—(Optional) For chassis cluster configurations, clear the specified session on a specific node (device) in the cluster.

- ***node-id***—Identification number of the node. It can be 0 or 1.
- **all**—Clear all nodes.
- **local**—Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session session-identifier on page 1391**

List of Sample Output

clear security flow session session-identifier 1 on page 1049
clear security flow session session-identifier 1 node 0 on page 1049

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session session-identifier 1

```
user@host> clear security flow session session-identifier 1
0 active sessions cleared
```

clear security flow session session-identifier 1 node 0

```
user@host> clear security flow session session-identifier 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session source-port

Syntax

clear security flow session source-port
source-port-number
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear each session that uses the specified source port.

Options

source-port-number —Number that identifies the source port.

Range: 1 through 65,535

node—(Optional) For chassis cluster configurations, clear sessions on the specified source port on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session source-port on page 1394**

List of Sample Output

clear security flow session source-port 1 on page 1050
clear security flow session source-port 1 node 0 on page 1050

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session source-port 1

```
user@host> clear security flow session source-port 1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session source-port 1 node 0

```
user@host> clear security flow session source-port 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2011, Juniper Networks, Inc.

clear security flow session source-prefix

Syntax

clear security flow session source-prefix
source-prefix-number
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS.
The **node** options added in Release 9.0 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.

Description

Clear sessions that match the source prefix.

Options

source-prefix-number—Source IP prefix or address.

node—(Optional) For chassis cluster configurations, clear security sessions matching the source prefix on a specific node (device) in the cluster.

- *node-id*—Identification number of the node. It can be 0 or 1.
- **all**—Clear all nodes.
- **local**—Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security flow session source-prefix on page 1398**

List of Sample Output

clear security flow session source-prefix 100.0.0.1 on page 1051
clear security flow session source-prefix 10::10 on page 1051
clear security flow session source-prefix 100.0.0.1 node 0 on page 1051

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security flow session source-prefix 100.0.0.1

```
user@host> clear security flow session source-prefix 100.0.0.1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session source-prefix 10::10

```
user@host> clear security flow session source-prefix 10::10
1 active sessions cleared
```

clear security flow session source-prefix 100.0.0.1 node 0

```
user@host> clear security flow session source-prefix 100.0.0.1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security gprs sctp counters

Syntax clear security gprs sctp counters

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear the statistics of the dropped Stream Control Transmission Protocol (SCTP) counters.

Options none—Clear all dropped SCTP counters.

Required Privilege Level clear

Related Documentation

- **show security gprs sctp counters on page 1415**

List of Sample Output **clear security gprs sctp counters on page 1052**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security gprs sctp counters

```
user@host> clear security gprs sctp counters
```


Copyright © 2011, Juniper Networks, Inc.

clear security group-vpn member ike security-associations

Syntax clear security group-vpn member ike security-associations [index *SA-index*] [*peer-ipaddress*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear IKE security association (SA) for a group member.

Options none—Clear all IKE SAs for the group member.

index—(Optional) Clear the IKE SA with this index number.

peer-ipaddress—(Optional) Clear the IKE SA with this peer.

Required Privilege Level clear

Related Documentation

- **show security group-vpn member ike security-associations on page 1416**

Output Fields This command produces no output.

clear security group-vpn member ike security-associations

```
user@host> clear security group-vpn member ike security-associations
```

clear security group-vpn member ipsec security-associations

Syntax clear security group-vpn member ipsec security-associations [index *SA-index*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear group VPN SA for a group member.

Options none—Clear all group VPN SAs for the group member.

index—(Optional) Clear the group VPN SA with this index number.

Required Privilege Level clear

Related Documentation

- **show security group-vpn member ipsec security-associations on page 1420**

Output Fields This command produces no output.

clear security group-vpn member ipsec security-associations

```
user@host> clear security group-vpn member ipsec security-associations
```


Copyright © 2011, Juniper Networks, Inc.

clear security group-vpn member kek security-associations

Syntax clear security group-vpn member kek security-assocations [index *SA-index*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear key encryption key (KEK) SAs for a group member.

Options none—Clear all KEK SAs for the group member.

index—(Optional) Clear the KEK SA with this index number.

Required Privilege Level clear

Related Documentation

- **show security group-vpn member kek security-associations on page 1423**

Output Fields This command produces no output.

clear security group-vpn member kek security-associations

```
user@host> clear security group-vpn member kek security-associations
```

clear security group-vpn server

Syntax clear security group-vpn server [group *group-name* | group-id *group-id*] [now]

Description Remove active members for a specified group. If no options are specified, members are removed from all groups. After this command is issued, members will need to reregister.

NOTE: An IKE SA can be used by a group member to register to multiple groups. When you remove members for a specified group, all existing IKE SAs that could be used to register to the group are also removed.

Options none—All members are removed from all groups.

group—(Optional) Remove members for the specified group name.

group-id—(Optional) Remove members for the specified group identifier.

now—(Optional) Immediatly remove all group-related information.

Required Privilege Level clear

Related Documentation

- **show security group-vpn server registered-members on page 1438**

Output Fields If there is a problem with the command, one of the following messages appears:

- Group does not exist
- Group is in the process of deletion
- Error in clear members
- Warning Message; Fail to push delete to members as server-member-communication is not configured.

clear security group-vpn server

```
user@host> clear security group-vpn server
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp

Syntax clear security idp
(application-identification | application-statistics | attack | counters | status)

Release Information Command introduced in Release 10.1 of Junos OS.

Description Clear the following IDP information:

- **application-identification**—Clear IDP application identification data.
- **application-statistics**—Clear IDP application statistics.
- **attack**—Clear IDP attack data
- **counters**—Clear IDP counters
- **status**—Clear IDP Status

Required Privilege Level clear

List of Sample Output **clear security idp status on page 1057**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp status

```
user@host> clear security idp status
Status of IDP: s0,      Up since: 2009-05-02 07:49:17 UTC (00:35:36 ago)

Packets/second: 0               Peak: 0 @ 2009-05-02 07:49:17 UTC
KBits/second  : 0               Peak: 0 @ 2009-05-02 07:49:17 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2009-05-02 07:49:17 UTC]
  TCP: [Current: 0] [Max: 0 @ 2009-05-02 07:49:17 UTC]
  UDP: [Current: 0] [Max: 0 @ 2009-05-02 07:49:17 UTC]
  Other: [Current: 0] [Max: 0 @ 2009-05-02 07:49:17 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]
  Policy Name : custom v0
  Running Detector Version : 9.2.160090324
```

Copyright © 2011, Juniper Networks, Inc.

clear security idp application-identification application-system-cache

Syntax clear security idp application-identification application-system-cache

Release Information Command introduced in Release 9.2 of Junos OS.

Description Clear IDP application system cache.

Required Privilege Level clear

Related Documentation

- **application-system-cache on page 349**
- **show security idp application-identification application-system-cache on page 1443**

List of Sample Output **clear security idp application-identification application-system-cache on page 1058**

Output Fields This command produces no output.

clear security idp application-identification application-system-cache

```
user@host> clear security idp application-identification application-system-cache
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp attack table

Syntax clear security idp attack table

Release Information Command introduced in Release 9.2 of Junos OS.

Description Clear details of the IDP attack table.

Required Privilege Level clear

Related Documentation

- **show security idp attack table on page 1444**

List of Sample Output **clear security idp attack table on page 1059**

Output Fields This command produces no output.

clear security idp attack table

```
user@host> clear security idp attack table
```

clear security idp counters application-identification

Syntax clear security idp counters application-identification

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the application identification counter values.

Required Privilege Level clear

Related Documentation

- application-identification on page 342
- show security idp counters application-identification on page 1448

List of Sample Output clear security idp counters application-identification on page 1060

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters application-identification

```
user@host> clear security idp counters application-identification
clear_counter_class: counters cleared, status = 0
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp counters dfa

Syntax clear security idp counters dfa

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the DFA counter values.

Required Privilege Level clear

Related Documentation

- show security idp counters dfa on page 1450

List of Sample Output clear security idp counters dfa on page 1061

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters dfa

```
user@host> clear security idp counters dfa
clear_counter_class: counters cleared, status = 0
```

clear security idp counters flow

Syntax clear security idp counters flow

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the IDP flow-related counter values.

Required Privilege Level clear

Related Documentation

- **flow (IDP) on page 457**
- **show security idp counters flow on page 1451**

List of Sample Output **clear security idp counters flow on page 1062**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters flow

```
user@host> clear security idp counters dfa
clear_counter_class: counters cleared, status = 0
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp counters ips

Syntax clear security idp counters ips

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the ips counter values.

Required Privilege Level clear

Related Documentation

- ips on page 532
- show security idp counters ips on page 1454

List of Sample Output clear security idp counters ips on page 1063

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters ips

```
user@host> clear security idp counters ips
clear_counter_class: counters cleared, status = 0
```

clear security idp counters log

Syntax clear security idp counters log

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the IDP log counter values.

Required Privilege Level clear

Related Documentation

- **event-rate on page 435**
- **show security idp counters log on page 1456**

List of Sample Output **clear security idp counters log on page 1064**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters log

```
user@host> clear security idp counters log
clear_counter_class: counters cleared, status = 0
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp counters packet

Syntax clear security idp counters packet

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the IDP packet counter values.

Required Privilege Level clear

Related Documentation

- show security idp counters packet on page 1459

List of Sample Output clear security idp counters packet on page 1065

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters packet

```
user@host> clear security idp counters packet
clear_counter_class: counters cleared, status = 0
```

clear security idp counters policy-manager

Syntax clear security idp counters policy-manager

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the IDP policies counter values.

Required Privilege Level clear

Related Documentation

- show security idp counters policy-manager on page 1464

List of Sample Output clear security idp counters policy-manager on page 1066

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters policy-manager

```
user@host> clear security idp counters policy-manager
clear_counter_class: counters cleared, status = 0
```


Copyright © 2011, Juniper Networks, Inc.

clear security idp counters tcp-reassembler

Syntax clear security idp counters tcp-reassembler

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reset all the TCP reassembler counter values.

Required Privilege Level clear

Related Documentation

- re-assembler on page 666
- show security idp counters tcp-reassembler on page 1465

List of Sample Output clear security idp counters tcp-reassembler on page 1067

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp counters tcp-reassembler

```
user@host> clear security idp counters tcp-reassembler
clear_counter_class: counters cleared, status = 0
```

clear security idp ssl-inspection session-id-cache

Syntax clear security idp ssl-inspection session-id-cache

Release Information Command introduced in Release 9.3 of Junos OS.

Description Clear all the entries stored in the SSL session ID cache.

Required Privilege Level clear

Related Documentation

- **show security idp ssl-inspection session-id-cache on page 1475**

List of Sample Output **clear security idp ssl-inspection session-id-cache on page 1068**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security idp ssl-inspection session-id-cache

```
user@host> clear security idp ssl-inspection session-id-cache
Total SSL session cache entries cleared : 2
```


Copyright © 2011, Juniper Networks, Inc.

clear security ike respond-bad-spi-count

Syntax

clear security ike respond-bad-spi-count
< *gateway-name* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Clear information about invalid Internet Key Exchange (IKE) security parameter index (SPI) counters.

Options

none—Clear all invalid SPI counters.

gateway-name —(Optional) Clear the invalid SPI counters for the given gateway.

Required Privilege Level

clear

Related Documentation

- **respond-bad-spi on page 672**

List of Sample Output

clear security ike respond-bad-spi-count on page 1069
clear security ike respond-bad-spi-count gateway-name1 on page 1069

Output Fields

This command produces no output.

clear security ike respond-bad-spi-count

`user@host>` **clear security ike respond-bad-spi-count**

clear security ike respond-bad-spi-count gateway-name1

`user@host>` **clear security ike respond-bad-spi-count gateway-name1**

clear security ike security-associations

Syntax

clear security ike security-associations
< *peer-address* >
< **port** >
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pic *slot-number*>
port
<family (inet | inet6)>

Release Information

Command introduced in Release 8.5 of Junos OS. The **fpc, pic,** and **kmd-instance** options added in Release 9.3 of Junos OS. The **port** option added in Release 10.0 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

Description

Clear information about the current Internet Key Exchange security associations (IKE SAs).

Options

none—Clear all IKE SAs.

peer-address —(Optional) Clear IKE SAs for the destination peer at this IP address.

fpc ***slot-number*** —Specific to SRX Series devices. Clear information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot.

index ***SA-index-number*** —(Optional) Clear the IKE SA with this index number.

port—(Optional) Port number of SA (1 through 65,535).

kmd-instance—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC ***slot-number*** and PIC ***slot-number***.

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- ***kmd-instance-name***—Name of the KMD instance running on the SPU.

pic ***slot-number*** —Specific to SRX Series devices. Clear information about existing IKE SAs in this PIC slot.

family—(Optional) Clear IKE SAs by family.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

Required Privilege Level

clear

Related Documentation

- **show security ike security-associations on page 1479**

Copyright © 2011, Juniper Networks, Inc.

List of Sample Output

clear security ike security-associations on page 1071
clear security ike security-associations 1.1.1.2 port 19405 on page 1071
clear security ike security-associations index 8 on page 1071
clear security ike security-associations family inet6 on page 1071
clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices) on page 1071

Output Fields

This command produces no output.

clear security ike security-associations

```
user@host> clear security ike security-associations
```

clear security ike security-associations 1.1.1.2 port 19405

```
user@host> clear security ike security-associations 1.1.1.2 port 19405
```

clear security ike security-associations index 8

```
user@host> clear security ike security-associations index 8
```

clear security ike security-associations family inet6

```
user@host> clear security ike security-associations family inet6
```

clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices)

```
user@host> clear security ike security-associations fpc 5 pic 0 kmd-instance all
```

clear security ipsec security-associations

Syntax

clear security ipsec security-associations
fpc *slot-number*
<index *SA-index-number*>
kmd-instance (all | *kmd-instance-name*)
pic *slot-number*
<family (inet | inet6)>

Release Information

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic,** and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

Description

Clear information about IPsec security associations (SAs).

Options

none—Clear all IPsec SAs.

fpc *slot-number* —Specific to SRX Series devices. Clear information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot.

index *SA-index-number* —(Optional) Clear the IPsec SA with this index number.

kmd-instance—Specific to SRX Series devices. Clear information about existing IPsec SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number* .

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- *kmd-instance-name*—Name of the KMD instance running on the SPU.

pic *slot-number* —Specific to SRX Series devices. Clear information about existing IPsec SAs in this PIC slot.

family—(Optional) Clear SAs by family.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

Required Privilege Level

clear

Related Documentation

- **show security ipsec security-associations on page 1486**

List of Sample Output

clear security ipsec security-associations on page 1072
clear security ipsec security-associations index 8 on page 1073
clear security ipsec security-associations family inet6 on page 1073

Output Fields

This command produces no output.

clear security ipsec security-associations

`user@host>` **clear security ipsec security-associations**

Copyright © 2011, Juniper Networks, Inc.

clear security ipsec security-associations index 8

```
user@host> clear security ipsec security-associations index 8
```

clear security ipsec security-associations family inet6

```
user@host> clear security ipsec security-associations family inet6
```

clear security ipsec statistics

Syntax

clear security ike statistics
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pic *slot-number*>

Release Information

Command introduced in Release 8.5 of Junos OS; **fpc and pic** options added in Release 9.3 of Junos OS ;**kmd-instance** option added in Release 10.4 of Junos OS.

Description

Clear IPsec statistics on the device.

Options

none—Clear all IPsec statistics.

fpc *slot-number* —Specific to SRX Series devices. Clear statistics about existing IPsec security associations (SAs) in this Flexible PIC Concentrator (FPC) slot.

index *SA-index-number* —(Optional) Clear the IPsec statistics for the SA with this index number.

kmd-instance—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number* .

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- *kmd-instance-name*—Name of the KMD instance running on the SPU.

pic *slot-number* —Specific to SRX Series devices. Clear statistics about existing IPsec SAs in this PIC slot.

Required Privilege Level

clear

Related Documentation

- **show security ipsec statistics on page 1492**

List of Sample Output

clear security ipsec statistics on page 1074
clear security ipsec statistics index 1 on page 1074
clear security ipsec statistics fpc 5 pic 0 (SRX Series devices) on page 1074

Output Fields

This command produces no output.

clear security ipsec statistics

```
user@host> clear security ipsec statistics
```

clear security ipsec statistics index 1

```
user@host> clear security ipsec statistics index 1
```

clear security ipsec statistics fpc 5 pic 0 (SRX Series devices)

```
user@host> clear security ipsec statistics fpc 5 pic 0
```


Copyright © 2011, Juniper Networks, Inc.

clear security nat incoming-table

Syntax

clear security nat incoming-table
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear Network Address Translation (NAT) incoming table information.

Options

none—Clear all information NAT incoming table.

node—(Optional) For chassis cluster configurations, clear incoming table information on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security nat incoming-table on page 1510**

List of Sample Output

clear security nat incoming-table on page 1075

Output Fields

This command produces no output.

clear security nat incoming-table

```
user@host> clear security nat incoming-table
```

clear security nat source persistent-nat-table

Syntax

clear security nat source persistent-nat-table
(all | interface | internal-ip *ip-address* <internal-port *port*> | pool *poolname*)

Release Information

Command introduced in Release 10.0 of Junos OS.

Description

Clear Network Address Translation (NAT) persistent NAT bindings that are in query mode, where all sessions of the binding are gone.

Options

all—Clear all persistent NAT bindings that are in query mode.

interface—Clear persistent NAT bindings that are in query mode for the specified interface.

internal-ip *ip-address*—Clear persistent NAT bindings for the specified internal IP address.

internal-ip *ip-address* internal-port *port*—Clear persistent NAT bindings that are in query mode for the specified internal IP address and port.

pool—Clear persistent NAT bindings that are in query mode for the specified source NAT pool.

Required Privilege Level

clear

Related Documentation

- Table 144 on page 1514

List of Sample Output

clear security nat source persistent-nat-table all on page 1076

Output Fields

This command produces no output.

clear security nat source persistent-nat-table all

```
user@host> clear security nat source persistent-nat-table all
```


Copyright © 2011, Juniper Networks, Inc.

clear security pki key-pair

Syntax clear security pki key-pair (all | certificate-id *certificate-id*)

Release Information Command introduced in Release 8.5 of Junos OS.

Description Clear public key infrastructure (PKI) key pair information for local digital certificates on the device.

Options **all**—Clear key pair information for all local certificates.

certificate-id ***certificate-id*** —Clear key pair information for the local certificate with this certificate ID.

Required Privilege Level clear and security

Related Documentation

- **show security pki certificate-request on page 1532**

List of Sample Output **clear security pki key-pair all on page 1077**

Output Fields This command produces no output.

clear security pki key-pair all

```
user@host> clear security pki key-pair all
```

clear security pki local-certificate

Syntax clear security pki local-certificate (all | certificate-id *certificate-id* | system-generated)

Release Information Command modified in Release 9.1 of Junos OS.

Description Clear public key infrastructure (PKI) information for local digital certificates on the device.

Options **all**—Clear information for all the local digital certificates on the device.

> NOTE: You cannot clear the automatically generated self-signed certificate using clear security pki local-certificate all command. To clear the self-signed certificate you need to use system-generated as an option.

certificate-id *certificate-id*—Clear the specified local digital certificate with this certificate ID.

system-generated—Clear the existing automatically generated self-signed certificate and generate a new self-signed certificate.

Required Privilege Level clear and security

Related Documentation

- **show security pki local-certificate on page 1536**
- **request security pki local-certificate generate-self-signed on page 1114**

List of Sample Output

clear security pki local-certificate all on page 1078
clear security pki local-certificate system-generated on page 1078

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

clear security pki local-certificate system-generated

```
user@host> clear security pki local-certificate system-generated
```


Copyright © 2011, Juniper Networks, Inc.

clear security policies statistics

Syntax clear security policies statistics

Release Information Command introduced in Release 8.5 of Junos OS.

Description Clear statistics for security policies configured on the device.

Required Privilege Level clear

Related Documentation

- **show security policies on page 1540**

List of Sample Output **clear security policies statistics on page 1079**

Output Fields This command produces no output.

clear security policies statistics

```
user@host> clear security policies statistics
```

clear security screen statistics

Syntax

clear security screen statistics
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 9.0 of Junos OS.

Description

Clear intrusion detection service (IDS) security screen statistics on the device.

Options

node—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security screen statistics on page 1553**

List of Sample Output

clear security screen statistics node 0 on page 1080

Output Fields

This command produces no output.

clear security screen statistics node 0

`user@host>` **clear security screen statistics node 0**

Copyright © 2011, Juniper Networks, Inc.

clear security screen statistics interface

Syntax clear security screen statistics interface *interface-name*

Release Information Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description Clear intrusion detection service (IDS) security screen statistics for an interface.

Options **interface** *interface-name* —Name of the interface on which to clear security screen statistics.

node—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level clear

Related Documentation
- **show security screen statistics on page 1553**

List of Sample Output
clear security screen statistics interface fab0 on page 1081
clear security screen statistics interface fab0 node 0 on page 1081

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear security screen statistics interface fab0

```
user@host> clear security screen statistics interface fab0
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
node1:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

clear security screen statistics interface fab0 node 0

```
user@host> clear security screen statistics interface fab0 node 0
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

clear security screen statistics zone

Syntax

clear security screen statistics zone *zone-name*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Clear IDS security screen statistics for a security zone.

Options

zone *zone-name* —Name of the security zone for which to clear security screen statistics.

node—(Optional) For chassis cluster configurations, clear security screen statistics for a security zone on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

Required Privilege Level

clear

Related Documentation

- **show security screen statistics on page 1553**

List of Sample Output

clear security screen statistics zone abc node all on page 1082
clear security screen statistics node 0 zone my-zone on page 1082

Output Fields

When you enter this command, you are provided feedback on the status of your request.

clear security screen statistics zone abc node all

```
user@host> clear security screen statistics zone abc node all
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
node1:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

clear security screen statistics node 0 zone my-zone

```
user@host> clear security screen statistics node 0 zone my-zone
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```


Copyright © 2011, Juniper Networks, Inc.

clear security utm anti-spam statistics

Syntax clear security utm anti-spam statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Clear antispam statistics information.

Required Privilege Level clear

Related Documentation

- **show security utm anti-spam statistics on page 1559**
- **show security utm anti-spam status on page 1560**

Output Fields This command produces no output.

clear security utm anti-spam statistics

```
user@host> clear security utm anti-spam statistics
```

clear security utm antivirus statistics

Syntax clear security utm anti-virus statistics

Release Information Command introduced in Release 9.5 of Junos OS. Support for Sophos Antivirus added in Release 11.1 of Junos OS.

Description Clear antivirus statistics information.

Required Privilege Level clear

Related Documentation

- **show security utm anti-virus statistics on page 1561**
- **show security utm anti-virus status on page 1562**
- **request security utm anti-virus juniper-express-engine on page 1117**
- **request security utm anti-virus kaspersky-lab-engine on page 1118**

Output Fields This command produces no output.

clear security utm antivirus statistics

```
user@host> clear security utm anti-virus statistics
```


Copyright © 2011, Juniper Networks, Inc.

clear security utm content-filtering statistics

Syntax clear security utm content-filtering statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Clear content-filtering statistics information.

Required Privilege Level clear

Related Documentation

- **show security utm content-filtering statistics on page 1564**

Output Fields This command produces no output.

clear security utm content-filtering statistics

```
user@host> clear security utm content-filtering statistics
```

clear security utm session

Syntax clear security utm session

Release Information Command introduced in Release 9.5 of Junos OS.

Description Clear UTM session information.

Required Privilege Level clear

Related Documentation

- **show security utm session on page 1565**
- **show security utm status on page 1566**

Output Fields This command produces no output.

clear security utm session

```
user@host> clear security utm session
```


Copyright © 2011, Juniper Networks, Inc.

clear security utm web-filtering statistics

Syntax clear security utm web-filtering statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Clear web filtering statistics information.

Required Privilege Level clear

Related Documentation

- **show security utm web-filtering statistics on page 1567**
- **show security utm web-filtering status on page 1568**

Output Fields This command produces no output.

clear security utm web-filtering statistics

```
user@host> clear security utm web-filtering statistics
```

clear services application-identification application-system-cache

Syntax clear services application-identification application-system-cache

Release Information Command introduced in Release 10.2 of Junos OS.

Description Clear Junos OS application identification application system cache.

Required Privilege Level clear

Related Documentation
- **show services application-identification application-system-cache on page 1577**

List of Sample Output **clear services application-identification application-system-cache on page 1088**

Output Fields This command produces no output.

clear services application-identification application-system-cache

```
user@host> clear services application-identification application-system-cache
```

 Copyright © 2011, Juniper Networks, Inc.

clear services application-identification counter

Syntax clear services application-identification counter

Release Information Command introduced in Release 10.2 of Junos OS.

Description Reset all the Junos OS application identification counter values.

Required Privilege Level clear

Related Documentation

- **show services application-identification counter on page 1579**

List of Sample Output **clear services application-identification counter on page 1089**

Output Fields When you enter this command, you are provided feedback on the status of your request.

clear services application-identification counter

```
user@host> clear services application-identification counter
clear_counter_class: counters cleared, status = 0
```

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 25

Request Commands

This section contains the following topics:

- Request Commands Overview on page 1091

Request Commands Overview

Use the **request** operational commands to stop or reboot device components, switch between primary and backup components, display messages, and display system information. Operational commands are organized alphabetically.

Related Documentation

- *Junos OS System Basics and Services Command Reference*.
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2011, Juniper Networks, Inc.

request services application-identification download

Syntax request services application-identification download <version>;

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Manually download and install the application package for Junos OS application identification. The application package is extraced from the IDP signature database and contains definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP.

Options **version**—(Optional) Download a specific version of the application package from the Juniper security web site. If you do not enter a version, the most recent version will be downloaded.

Required Privilege Level maintenance

List of Sample Output **request services application-identification download on page 1092**

Output Fields When you enter this command, you are provided feedback on the status of your request.

request services application-identification download

```
user@host> request services application-identifications download
application package 1608 downloaded successfully and is installing.
```

 Copyright © 2011, Juniper Networks, Inc.

request services application-identification download status

Syntax request services application-identification download status;

Release Information Statement introduced in Release 10.2 of Junos OS.

Description Check the download status of the application identification signature package.

Required Privilege Level maintenance

List of Sample Output **request services application-identification download status on page 1093**

Output Fields When you enter this command, you are provided feedback on the status of your request.

request services application-identification download status

```
user@host> request services application-identifications download status
Application package 1608 installation is in progress.

Application package 1608 installed successfully.
```

request services application-identification uninstall

Syntax request services application-identification uninstall [all | predefined | customer-defined];

Release Information Statement introduced in Release 10.2 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

Description Uninstall from your configuration the predefined application definition package for application identification services, all custom application definitions that you have created, or both.

Options

all—Uninstall from your configuration both the predefined application definition package and all custom application definitions that you have created.

customer-defined—Uninstall from your configuration all custom application definitions that you created, but maintain the predefined application definition package.

predefined—(Default) Uninstall from your configuration the predefined application definition package, but maintain all custom application definitions that you have created.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

```
user@host> request services application-identification uninstall
application package 1608 is uninstalled successfully.
```

```
user@host> request services application-identification uninstall predefined
application package 1608 is uninstalled successfully.
```

```
user@host> request services application-identification uninstall customer-defined
customer defined applications are uninstalled successfully.
```

```
user@host> request services application-identification uninstall all
application package 1608 and customer defined applications are uninstalled
successfully.
```


Copyright © 2011, Juniper Networks, Inc.

request chassis cluster failover node

Syntax

request chassis cluster failover node *node-number*
redundancy-group *group-number*

Release Information

Command introduced in Release 9.0 of Junos OS.

Description

For chassis cluster configurations, initiate manual failover in a redundancy group from one node to the other, which becomes the primary node, and automatically reset the priority of the group to 255. The failover stays in effect until the new primary node becomes unavailable, the threshold of the redundancy group reaches 0, or you use the **request chassis cluster failover reset** command.

After a manual failover, you must use the **request chassis cluster failover reset** command before initiating another failover.

Options

node *node-number*-Number of the chassis cluster node to which the redundancy group fails over.

Range: 0 through 1

redundancy-group *group-number* —Number of the redundancy group on which to initiate manual failover. Redundancy group 0 is a special group consisting of the two Routing Engines in the chassis cluster.

Range: 0 through 255

Required Privilege Level

maintenance

Related Documentation

- **clear chassis cluster failover-count on page 1004**
- **request chassis cluster failover reset on page 1096**
- **show chassis cluster status on page 1157**

List of Sample Output

request chassis cluster failover node 0 redundancy-group 1 on page 1095

Output Fields

This command produces no output.

request chassis cluster failover node 0 redundancy-group 1

```
user@host> request chassis cluster failover node 0 redundancy-group 1
```

request chassis cluster failover reset

Syntax

request chassis cluster failover reset
redundancy-group *group-number*

Release Information

Command introduced in Release 9.0 of Junos OS.

Description

In chassis cluster configurations, undo the previous manual failover and return the redundancy group to its original settings.

Options

redundancy-group ***group-number*** —Number of the redundancy group on which to reset manual failover. Redundancy group 0 is a special group consisting of the two Routing Engines in the chassis cluster.

Range: 0 through 255

Required Privilege Level

maintenance

Related Documentation

- **clear chassis cluster failover-count on page 1004**
- **request chassis cluster failover node on page 1095**
- **show chassis cluster status on page 1157**

List of Sample Output

request chassis cluster failover reset redundancy-group 0 on page 1096

Output Fields

This command produces no output.

request chassis cluster failover reset redundancy-group 0

```
user@host> request chassis cluster failover reset redundancy-group 0
```


Copyright © 2011, Juniper Networks, Inc.

request modem wireless activate iota

Syntax request modem wireless activate iota *interface-name*

Release Information Command introduced in Release 9.5 of Junos OS.

Description For CDMA EV-DO 3G wireless modem interfaces, enable modem card to connect to service provider's cellular network using Internet-based over the air (IOTA) provisioning.

Options ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request modem wireless activate iota cl-0/0/8

```
user@host> request modem wireless activate iota cl-0/0/8
Beginning IOTA Activation. It can take up to 5 minutes
Please check the trace logs for details.
```

request modem wireless activate manual

Syntax

request modem wireless activate manual *interface-name* msl *msl-number* mdn *mdn-number* imsi *imsi-number* sid *sid-number* nid *nid-number* sip-user-id *sip-id* sip-password *sip-password*

Release Information

Command introduced in Release 9.5 of Junos OS.

Description

For CDMA EV-DO 3G wireless modem interfaces, enable modem card to connect to service provider's cellular network.

Options

interface-name—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

msl *msl-number*—Master subsidy lock (MSL) number required to unlock the modem card. Obtain the number from the service provider.

mdn *mdn-number*—Mobile directory number (MDN) 10–digit phone number. Obtain the number from the service provider.

imsi *imsi-number*—International mobile station identity (IMSI) subscriber identification number. Obtain the number from the service provider.

sid *sid-number*—System identification (SID) number. Use the **show modem wireless interface network** command to display the SID.

nid *nid-number*—Network identification (NID) number. Use the **show modem wireless interface network** command to display the NID.

sip-user-id *sip-id*—Simple IP user identification. Obtain the username from the service provider.

sip-password *sip-password*—Simple IP password. Obtain the password from the service provider.

Required Privilege Level

maintenance

Related Documentation

- **show modem wireless interface network on page 1226**

Output Fields

When you enter this command, you are provided feedback on the status of your request.

request modem wireless activate manual cl-0/0/8 msl 43210 mdn 0123456789 imsi 0123456789 sid 12345 nid 12345 sip-usr-id jnpr sip-password jn9r1

```
user@host> request modem wireless activate manual cl-0/0/8 msl 43210 mdn 0123456789
imsi 0123456789 sid 12345 nid 12345 sip-usr-id jnpr sip-password jn9r1
Checking status...
 Modem current activation status: Not Activated
Starting activation...
 Performing account activation step 1/6 : [Unlock] Done
 Performing account activation step 2/6 : [Set MDN] Done
 Performing account activation step 3/6 : [Set SIP Info] Done
 Performing account activation step 4/6 : [Set IMSI] Done
 Performing account activation step 5/6 : [Set SID/NID] Done
 Performing account activation step 6/6 : [Commit/Lock] Done
Configuration Commit Result: PASS
```


Copyright © 2011, Juniper Networks, Inc.

```
Resetting the modem ... Done
Account activation in progress. It can take up to 5 minutes
Please check the trace logs for details.
```

request modem wireless activate otasp

Syntax request modem wireless activate otasp *interface-name* dial-string *calling-number*

Release Information Command introduced in Release 9.5 of Junos OS.

Description For CDMA EV-DO 3G wireless modem interfaces, enable the modem card to connect to service provider's cellular network using over-the-air service provisioning (OTASP).

Options ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

dial-string *calling-number*—Dial number that the modem uses to contact the network. Obtain the number from the service provider.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request modem wireless activate otasp cl-0/0/8 dial-string *22864

```
user@host> request modem wireless activate otasp cl-0/0/8 dial-string *22864
OTASP number *22286*, Selecting NAM 0
Beginning OTASP Activation. It can take up to 5 minutes
Please check the trace logs for details.
```


Copyright © 2011, Juniper Networks, Inc.

request modem wireless gsm sim-unblock

Syntax request modem wireless gsm sim-unblock *interface-name* puk *unblock-code*

Release Information Command introduced in Release 9.5 of Junos OS.

Description Unblock a blocked subscriber identity module (SIM) in the GSM 3G wireless modem card.

Options ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

puk *unblock-code*—Eight-digit PIN unblocking key (PUK). Obtain the PUK from the service provider.

NOTE: If the PUK is entered incorrectly ten times, the SIM must be returned to the service provider for reactivation.

Required Privilege Level maintenance

Related Documentation

- **request modem wireless gsm sim-unlock on page 1102**

Output Fields When you enter this command, you are provided feedback on the status of your request.

request modem wireless gsm sim-unblock cl-0/0/8 puk 76543210

```
user@host> request modem wireless gsm sim-unblock cl-0/0/8 puk 76543210
Issued SIM unblock request successfully.
Please verify SIM lock status under firmware stats
```

request modem wireless gsm sim-unlock

Syntax request modem wireless gsm sim-unlock *interface-name* pin *unlock-code*

Release Information Command introduced in Release 9.5 of Junos OS.

Description Unlock the subscriber identity module (SIM) in the GSM 3G wireless modem card.

Options ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

pin *unlock-code*—Four-digit personal identification number (PIN). Obtain the PIN from the service provider.

NOTE: If the PIN is entered incorrectly three consecutive times, the SIM is blocked. Obtain a PIN unblocking key (PUK) from the service provider.

Required Privilege Level maintenance

Related Documentation

- **request modem wireless gsm sim-unblock on page 1101**

Output Fields When you enter this command, you are provided feedback on the status of your request.

request modem wireless gsm sim-unlock cl-0/0/8 pin 3210

```
user@host> request modem wireless gsm sim-unlock cl-0/0/8 pin 3210
Issued SIM unlock request successfully.
Please verify SIM lock status under firmware stats
```


Copyright © 2011, Juniper Networks, Inc.

request security datapath-debug capture start

Syntax request security datapath-debug capture start

Release Information Command introduced in Release 10.0 of Junos OS.

Description Start the data path debugging capture.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request security datapath-debug capture start

```
user@host> request security datapath-debug capture start
datapath-debug capture started on file
```

request security datapath-debug capture stop

Syntax request security datapath-debug capture stop

Release Information Command introduced in Release 10.0 of Junos OS.

Description Stop the data path debugging capture.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request security datapath-debug capture stop

```
user@host> request security datapath-debug capture stop
datapath-debug capture successfully stopped, use show security datapath-debug
capture to view
```


Copyright © 2011, Juniper Networks, Inc.

request security idp security-package download

Syntax

request security idp security-package download
<check-server>
<full-update>
<policy-templates>
<version *version-number* >
<status>

Release Information

Command introduced in Release 9.2 of Junos OS. Detailed status added in Release 10.1 of Junos OS. Description modified in Release 11.1 of Junos OS.

Description

Manually download the individual components of the security package from the Juniper Security Engineering portal. The components are downloaded into a staging folder inside the device.

By default, this command tries to download the delta set attack signature table. It also downloads both IDP and IPS signatures.

Options

check-server—(Optional) Retrieve the version information of the latest security package from the security portal server.

full-update—(Optional) Download the latest security package with the full set of attack signature tables from the portal.

policy-templates—(Optional) Download the latest policy templates from the portal.

version ***version-number*** —(Optional) Download the security package of a specific version from the portal.

status—(Optional) Provided detailed status of security package download operation.

Required Privilege Level

maintenance

Related Documentation

- **show security idp active-policy on page 1440**
- **show security idp security-package-version on page 1473**

List of Sample Output

request security idp security-package download on page 1105
request security idp security-package download policy-templates on page 1106
request security idp security-package download version 1151 full-update on page 1106
request security idp security-package download status on page 1106

Output Fields

When you enter this command, you are provided feedback on the status of your request.

request security idp security-package download

```
user@host> request security idp security-package download
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1152(Thu Apr 24 14:37:44 2008, Detector=9.1.140080400)
```

request security idp security-package download policy-templates

```
user@host> request security idp security-package download policy-templates
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:35
```

request security idp security-package download version 1151 full-update

```
user@host> request security idp security-package download version 1151 full-update
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1151(Wed Apr 23 14:39:15 2008, Detector=9.1.140080400)
```

request security idp security-package download status

To request status for a package download:

```
user@host> request security idp security-package download status
In progress: SignatureUpdate_tmp.xml.gz      107169 bytes/ 10 MB
```

To request status for a template download:

```
user@host> request security idp security-package download status
Done; Successfully downloaded from
(https://devdb.secteam.juniper.net/xmlexport.cgi).
```


Copyright © 2011, Juniper Networks, Inc.

request security idp security-package install

Syntax

request security idp security-package install
<policy-templates>
<status>
<update-attack-database-only>

Release Information

Command introduced in Release 9.2 of Junos OS. Description modified in Release 11.1 of Junos OS.

Description

Update the attack database inside the device with the newly downloaded one from the staging folder, recompiles the existing running policy and pushes the re-compiled policy to the data plane.

Also, if there is an existing running policy and the previously installed detector's version is different from the newly downloaded one, the downloaded components are pushed to the data plane. This command install both IDP and IPS signatures.

Options

policy-templates—(Optional) Install the policy template file into /var/db/scripts/commit/templates.

status—(Optional) The command **security-package install** may take long time depending on the new Security DB size. Hence, **security-package install** command returns immediately and a background process performs the task. So, user can check the status using **security-package install status** command.

update-attack-database-only—(Optional) Loads the security package into IDP database but do not compile/push the active policy or the new detector to the data plane.

Required Privilege Level

maintenance

Related Documentation

- **show security idp active-policy on page 1440**
- **show security idp security-package-version on page 1473**

List of Sample Output

request security idp security-package install on page 1107
request security idp security-package install status on page 1107

Output Fields

When you enter this command, you are provided feedback on the status of your request.

request security idp security-package install

```
user@host> request security idp security-package install
Will be processed in async mode. Check the status using the status checking CLI
```

request security idp security-package install status

To request status on a package installation:

```
user@host> request security idp security-package install status
Done;Attack DB update : successful - [UpdateNumber=1152,ExportDate=Thu Apr 24
14:37:44 2008]
```

```
    Updating data-plane with new attack or detector : not performed
    due to no existing active policy found.
```

To request status on a template installation:

```
user@host> request security idp security-package install status
Done; policy-template has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```


Copyright © 2011, Juniper Networks, Inc.

request security idp ssl-inspection key add

Syntax

request security idp ssl-inspection key add *<key-name>* [file *<file-name>*] [password *<password-string>*] [server *<server-ip>*]

Release Information

Command introduced in Release 9.3 of Junos OS.

Description

Install a Privacy-Enhanced Mail (PEM) key that is optionally password protection, and associate a server with an installed key. The length of each key name and password string should not exceed 32 alpha-numeric characters long.

Options

key-name—Name of the SSL private key.

file *<file-name>*—(Optional) Location of RSA private key (PEM format) file.

password *<password-string>*—(Optional) Password used to encrypt specified key.

server *<server-ip>* —(Optional) Server IP address to be added to the specified key.

Required Privilege Level

maintenance

Related Documentation

- show security idp ssl-inspection key on page 1474

List of Sample Output

request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted on page 1109
request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted on page 1109
request security idp ssl-inspection key add key3 file /var/tmp/norm.key on page 1109
request security idp ssl-inspection key add key1 server 1.1.0.1 on page 1110
request security idp ssl-inspection key add key1 server 1.1.0.2 on page 1110

Output Fields

When you enter this command, you are provided feedback on the status of your request.

request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted

```
user@host> request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password
encrypted
Added key 'key1'
```

request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted

```
user@host> request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password
encrypted
Added key 'key2', server 2.2.0.1
```

request security idp ssl-inspection key add key3 file /var/tmp/norm.key

```
user@host> request security idp ssl-inspection key add key3 file /var/tmp/norm.key
Added key 'key3'
```

request security idp ssl-inspection key add key1 server 1.1.0.1

```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.1
Added key 'key1', server 1.1.0.1
```

request security idp ssl-inspection key add key1 server 1.1.0.2

```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.2
Added key 'key1', server 1.1.0.2
```


Copyright © 2011, Juniper Networks, Inc.

request security idp ssl-inspection key delete

Syntax request security idp ssl-inspection key delete [*<key-name>* [server *<server-ip>*]]

Release Information Command introduced in Release 9.3 of Junos OS.

Description Delete the specified server IP from the given key if the server is specified. If the server IP is not specified, the given key will be deleted along with all the server addresses associated with it.

NOTE: You will get a delete confirmation question before deleting one or more keys or server.

Options *key-name*—(Optional) Name of the SSL private key.

server *<server-ip>* —(Optional) Server IP address associated with the specified key to be deleted.

Required Privilege Level maintenance

Related Documentation

- show security idp ssl-inspection key on page 1474

List of Sample Output

request security idp ssl-inspection key delete on page 1111
request security idp ssl-inspection key delete key1 on page 1111
request security idp ssl-inspection key delete key2 server 2.2.0.1 on page 1111

Output Fields When you enter this command, you are provided feedback on the status of your request.

request security idp ssl-inspection key delete

```
user@host> request security idp ssl-inspection key delete

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes

Number of keys 4, server 3 deleted
```

request security idp ssl-inspection key delete key1

```
user@host> request security idp ssl-inspection key delete key1

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes

Number of keys 1, server 2 deleted
```

request security idp ssl-inspection key delete key2 server 2.2.0.1

```
user@host> request security idp ssl-inspection key delete key2 server 2.2.0.1

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes
```

Copyright © 2011, Juniper Networks, Inc.

```
Number of keys 0, server 1 deleted
```


Copyright © 2011, Juniper Networks, Inc.

request security pki ca-certificate verify

Syntax **request security pki ca-certificate verify ca-profile** ***ca-profile-name***

Release Information Command introduced in Release 8.5 of Junos OS.

Description Verify the digital certificate installed for the specified certificate authority (CA).

Options **ca-profile** ***ca-profile-name*** —Display the specified CA profile.

Required Privilege Level maintenance and security

Related Documentation

- **ca-profile on page 365**
- **show security pki ca-certificate on page 1528**

List of Sample Output

request security pki ca-certificate verify ca-profile ca1 (CRL downloaded) on page 1113
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded) on page 1113

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output This user has downloaded the certificate revocation list (CRL).

request security pki ca-certificate verify ca-profile ca1 (CRL downloaded)

```
user@host> request security pki ca-certificate verify ca-profile ca1
CA certificate ca1 verified successfully
```

Sample Output This user has not downloaded the certificate revocation list (CRL).

request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)

```
user@host> request security pki ca-certificate verify ca-profile ca1
CA certificate ca1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

request security pki local-certificate generate-self-signed

Syntax

request security pki local-certificate generate-self-signed

certificate-id ***certificate-id-name***

domain-name ***domain-name*** **subject** ***subject-distinguished-name***

<email ***email-address>***

<ip-address ***ip-address***>

Release Information

Command introduced in Release 9.1 of Junos OS.

Description

Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id ***certificate-id-name***—Name of the certificate and the public/private key pair.

domain-name ***domain-name***—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

subject ***subject-distinguished-name***—Distinguished name format that contains the common name, department, company name, state, and country in the following format: CN, OU, O, ST, C

- CN—Common name
- OU—Organizational unit name
- O—Organization name
- ST—State
- C—Country

email ***email-address***—E-mail address of the certificate holder.

ip-address ***ip-address***—IP address of the routing platform.

Required Privilege Level

maintenance and security

Related Documentation

- **clear security pki local-certificate on page 1078**
- **show security pki local-certificate on page 1536**

List of Sample Output

request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name juniper.net email mholmes@juniper.net on page 1115

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Copyright © 2011, Juniper Networks, Inc.

request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name juniper.net email mholmes@juniper.net

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name juniper.net email mholmes@juniper.net
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate verify

Syntax request security pki local-certificate verify certificate-id *certificate-id-name*

Release Information Command introduced in Release 8.5 of Junos OS.

Description Verify the validity of the local digital certificate identifier.

Options **certificate-id** *certificate-id-name* — Name of the local digital certificate identifier.

Required Privilege Level maintenance and security

List of Sample Output
request security pki local-certificate verify certificate-id bme1 (not downloaded) on page 1116
request security pki local-certificate verify certificate bme1 (downloaded) on page 1116

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output You receive the following response before the certificate revocation list (CRL) is downloaded:

request security pki local-certificate verify certificate-id bme1 (not downloaded)

```
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1: CRL verification in progress. Please check the PKId debug
 logs for completion status
```

Sample Output You receive the following response after the certificate revocation list (CRL) is downloaded:

request security pki local-certificate verify certificate bme1 (downloaded)

```
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1 verification success
```


Copyright © 2011, Juniper Networks, Inc.

request security utm anti-virus juniper-express-engine

Syntax request security utm anti-virus juniper-express-engine

Release Information Command introduced in Release 9.5 of Junos OS.

Description Manually update the express antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually.

Options **pattern-delete** — Delete the current express antivirus pattern database.

pattern-reload — Reload the express antivirus pattern database.

pattern-update — Update the express antivirus pattern database with the latest signatures.

Required Privilege Level maintenance

Related Documentation

- **request security utm anti-virus kaspersky-lab-engine on page 1118**
- **clear security utm antivirus statistics on page 1084**
- **show security utm anti-virus statistics on page 1561**
- **show security utm anti-virus status on page 1562**

Output Fields request security utm anti-virus juniper-express-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

request security utm anti-virus juniper-express-engine pattern-update

```
user@host> request security utm anti-virus juniper-express-engine pattern-update
```

request security utm anti-virus kaspersky-lab-engine

Syntax

request security utm anti-virus kaspersky-lab-engine

Release Information

Description

Manually update the full file-based antivirus pattern database using the commands described. You can update the full file-based antivirus pattern database automatically or manually.

Options

pattern-delete — Delete the current full file-based antivirus pattern database.

pattern-reload — Reload the full file-based antivirus pattern database.

pattern-update — Update the full file-based antivirus pattern database with the latest signatures.

Required Privilege Level

maintenance

Related Documentation

- **request security utm anti-virus juniper-express-engine on page 1117**
- **clear security utm antivirus statistics on page 1084**
- **show security utm anti-virus statistics on page 1561**
- **show security utm anti-virus status on page 1562**

Output Fields

request security utm anti-virus kaspersky-lab-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

request security utm anti-virus kaspersky-lab-engine pattern-update

```
user@host> request security anti-virus kaspersky-lab-engine pattern-update
```


Copyright © 2011, Juniper Networks, Inc.

request security utm anti-virus sophos-engine

Syntax

request security utm anti-virus sophos-engine

Release Information

Command introduced in Release 11.1 of Junos OS.

Description

Manually update the Sophos antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually. To update automatically you use the configuration statement **set security utm feature-profile anti-virus sophos-engine pattern-update interval *seconds***.

Options

pattern-delete — Delete the current Sophos antivirus pattern database.

pattern-reload — Reload the Sophos antivirus pattern database.

pattern-update — Update the Sophos antivirus pattern database with the latest signatures.

Required Privilege Level

maintenance

Related Documentation

- **clear security utm antivirus statistics on page 1084**
- **show security utm anti-virus statistics on page 1561**
- **show security utm anti-virus status on page 1562**

Output Fields

request security utm anti-virus sophos-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

request security utm anti-virus sophos-engine pattern-update

```
user@host> request security utm anti-virus sophos-engine pattern-update
```

request system license update

Syntax request system license update

Release Information Command introduced in Release 9.5 of Junos OS.

Description Starts autoupdating license keys from the LMS server.

This command is supported on J-series devices.

Options **trial**—Starts autoupdating trial license keys from LMS server.

Required Privilege Level maintenance

List of Sample Output **request system license update on page 1120**
request system license update trial on page 1120

Output Fields When you enter this command, you are provided feedback on the status of your request.

request system license update

```
user@host> request system license update

Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial

Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

 Copyright © 2011, Juniper Networks, Inc.

request system partition compact-flash

Syntax request system partition compact-flash

Release Information Command introduced in Release 9.2 of Junos OS.

Description Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.

Required Privilege Level maintenance

List of Sample Output **request system partition compact-flash (If Yes) on page 1121**
request system partition compact-flash (If No) on page 1121

Output Fields When you enter this command, you are provided feedback on the status of your request.

request system partition compact-flash (If Yes)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>
```

request system partition compact-flash (If No)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no
```

request system services dhcp

Syntax request system services dhcp (release *interface-name* | renew *interface-name)*

Release Information Command introduced in Release 8.5 of Junos OS.

Description Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the **show system services dhcp client** *interface-name* command.

Options **release** *interface-name* —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.

renew *interface-name* —Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.

Required Privilege Level maintenance

Related Documentation

- **dhcp on page 162**
- **show system services dhcp client on page 1586**

List of Sample Output **request system services dhcp client release ge-1/0/1 on page 1122**
request system services dhcp client renew ge-1/0/1 on page 1122

Output Fields This command produces no output.

request system services dhcp client release ge-1/0/1

```
user@host> request system services dhcp client release ge-1/0/1
```

request system services dhcp client renew ge-1/0/1

```
user@host> request system services dhcp client renew ge-1/0/1
```

 Copyright © 2011, Juniper Networks, Inc.

request system snapshot partition

Syntax request system snapshot partition

Release Information Command introduced in Release 10.2 of Junos OS.

Description Back up the currently running and active file system partitions on the device to standby partitions that are not running.

Options

- factory— Specifies that the only files shipped from factory are included in snapshot
- media— Specifies the media for snapshot:
  - internal— Reboots from the internal media. This is the default.
  - usb— Reboots from the USB storage device.
  - external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.
- slice— Specifies the partition for snapshot:
  - alternate— Alternate partition.

Required Privilege Level maintenance

Example **user@host# request system snapshot partition media internal factory slice alternate**

request system software add

Syntax request system software add *package-name*

Release Information Partition option introduced in the command in Release 10.1. of Junos OS.

Description Installs the new software package on the device.

Options

- delay–restart — Installs the software package but does not restart the software process
- best-effort-load— Activate a partial load and treat parsing errors as warnings instead of errors
- no-copy — Installs the software package but does not saves the copies of package files
- no-validate— Does not check the compatibility with current configuration before installation starts
- partition — Formats and re-partitions the media before installation
- reboot— Reboots the device after installation is completed
- unlink—Removes the software package after successful installation
- validate—Checks the compatibility with current configuration before installation starts

Required Privilege Level maintenance

Example **user@host# request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot**

Copyright © 2011, Juniper Networks, Inc.

request system software in-service-upgrade

Syntax request system software in-service-upgrade *image_name* *<no-old-master-upgrade>*

Release Information Command introduced in Release 9.6 of Junos OS.

Description The in-service software upgrade (ISSU) feature allows a chassis cluster pair to be upgraded or downgraded from supported Junos OS versions with a traffic impact similar to that of redundancy group failovers. Before upgrading, you should perform failovers so that all redundancy groups are active on only one device. We recommend that routing protocols graceful restart be enabled prior to initiating an ISSU.

Options ***image_name***—This is the location and name of the software upgrade package to be installed.

no-old-master-upgrade—(optional) This switch leaves the current master device in a nonupgraded state, which is a precaution against service failure. This option allows routing control to be quickly returned to the old master device if the newly upgraded device does not operate correctly.

Use of the **no-old-master-upgrade** option will require you to run a standard upgrade on the old master device after the ISSU is completed on the backup device.

NOTE: We recommend that in running this command, you include **reboot** at the end of the command sequence. If **reboot** is not included in the command, you will need to manually reboot each device as the ISSU completes updating the software image.

Required Privilege Level maintenance

List of Sample Output **request system software in-service-upgrade reboot on page 1125**

Output Fields When you enter this command, you are provided feedback on the status of your request.

request system software in-service-upgrade reboot

```
user@host> request system software in-service-upgrade
/var/tmp/junos-srx3000–9.6R1.13-domestic.tgz reboot
Chassis ISSU Started
node0:
--------------------------------------------------------------------------
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade

node0:
--------------------------------------------------------------------------
Initiating in-service-upgrade
Checking compatibility with configuration
Initializing...
Using /var/tmp/junos-srx3000-9.6R1.13-domestic.tgz
```

```
Checking junos requirements on /
Available space: 229192 require: 4102
Verified SHA1 checksum of issu-indb.tgz
Verified junos-boot-srx3000-9.6R1.13.tgz signed by PackageDevelopment_9_6_0
Verified junos-srx3000-9.6R1.13-domestic signed by PackageDevelopment_9_6_0
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded

Pushing bundle to node0
Installing package '/var/tmp/junos-srx3000-9.6R1.13-domestic.tgz' ...
Verified SHA1 checksum of issu-indb.tgz
Verified junos-boot-srx3000-9.6R1.13.tgz signed by PackageDevelopment_9_6_0
Verified junos-srx3000-9.6R1.13-domestic signed by PackageDevelopment_9_6_0
Available space: 391052 require: 175814
Verified SHA1 checksum of issu-indb.tgz
Verified junos-boot-srx3000-9.6R1.13.tgz signed by PackageDevelopment_9_6_0
Verified junos-srx3000-9.6R1.13-domestic signed by PackageDevelopment_9_6_0
JUNOS 9.6R1.13 will become active at next reboot
WARNING: A reboot is required to load this software correctly
WARNING:     Use the 'request system reboot' command
WARNING:         when software installation is complete
Saving package file in /var/sw/pkg/junos-9.6R1.13.tgz ...
Saving state for rollback ...
Finished upgrading secondary node node0
Rebooting Secondary Node

node0:
--------------------------------------------------------------------------
Shutdown NOW!
[pid 1365]
ISSU: Backup RE Prepare Done
Waiting for node0 to reboot.

node0 booted up.
Waiting for node0 to become secondary

node0 became secondary.
```


Copyright © 2011, Juniper Networks, Inc.

request system software reboot

Syntax request system software reboot *<at time> <in minutes><media><message 'text">*

Release Information Command introduced in Release 10.1 of Junos OS.

Description Reboots the software.

Options

- at time— Specifies the time at which to reboot the device . You can specify time in one of the following ways:
  - now— Reboots the device immediately. This is the default.
  - +minutes— Reboots the device in the number of minutes from now that you specify.
  - yymmddhhmm— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
  - hh:mm— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
- in minutes — Specifies the number of minutes from now to reboot the device. This option is a synonym for the at +minutes option
- media type— Specifies the boot device to boot the device from:
  - internal— Reboots from the internal media. This is the default.
  - usb— Reboots from the USB storage device.
  - external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.
- message "text"— Provides a message to display to all system users before the device reboots.

Required Privilege Level maintenance

Example **user@host# request system reboot at 5 in 50 media internal message stop**

request system software rollback

Syntax request system software rollback

Release Information Command introduced in Release 10.1 of Junos OS.

Description Revert to the software that was loaded at the last successful **request system software add** command.

Required Privilege Level maintenance

Example **user@host# request system software rollback**

Copyright © 2011, Juniper Networks, Inc.

request wan-acceleration login

Syntax request wan-acceleration login fpc *slot-number*

Release Information Command introduced in Release 8.5 of Junos OS.

Description Log in to the WXC Integrated Services Module (ISM 200) from J Series devices running Junos OS to access the WXOS CLI.

To view the slot number, enter the **show chassis fpc pic-status** command. You require interface permission for read-only access, and interface-control and configure permission for read-write access.

Options **fpc** *slot-number* —Higher number of the two slots in the device chassis occupied by the WXC ISM 200.

Required Privilege Level maintenance

Related Documentation

- **show chassis fpc on page 1163**
- **show wan-acceleration status on page 1593**

List of Sample Output

request wan-acceleration login fpc 3 (permissions set) on page 1129
request wan-acceleration login fpc 3 (permissions not set) on page 1129

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output This user has a user account with interface-control and configure permissions set for read-write access to WXOS or has interface permissions set for read-only access.

request wan-acceleration login fpc 3 (permissions set)

```
user@host> request wan-acceleration login fpc 3
Copyright 2001-2006 Juniper Networks, Inc. All Rights Reserved.
```

Sample Output This user has a user account without the correct permissions set and does not gain access to WXOS.

request wan-acceleration login fpc 3 (permissions not set)

```
user@host> request wan-acceleration login fpc 3
FPCLOGIN_LOGIN_FAILURE: fpclogin failed: user permissions not set.
```

request wlan access-point firmware upgrade

Syntax request wlan access-point firmware upgrade (*name* | all) file *image*

Release Information Command introduced in Release 10.0 of Junos OS.

Description Upgrade access point software.

Options *name*—Upgrade software on a specific access point on the services gateway.

all—Upgrade software on all access points on the services gateway.

file—Software to be upgraded onto the access point(s).

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request wlan access-point firmware upgrade wap-3

```
user@host> request wlan access-point firmware upgrade wap-3 file
/var/tmp/upgrade_10_1_0_1.tar
Firmware upgraded initiated for access point wap-3.
Upgrade will take approximately 6 minutes.
Access point will be unavailable during upgrade.
Please do not power down the access point while upgrade is in progress.
```

request wlan access-point firmware upgrade all

```
user@host> request wlan access-point firmware upgrade all file /var/tmp/upgrade_10_1_0_1.tar
Firmware upgraded initiated for all access points .
```


Copyright © 2011, Juniper Networks, Inc.

request wlan access-point firmware switch image

Syntax request wlan access-point firmware switch-image *name*

Release Information Command introduced in Release 11.1 of Junos OS.

Description Switch to alternate firmware image on the access point.

Options ***name*** — Access point on which the alternate firmware is requested.

Required Privilege Level maintenance

Example **user@host# request wlan access-point firmware switch-image mav-ap**

request wlan access-point restart

Syntax request wlan access-point restart *name*

Release Information Command introduced in Release 10.0 of Junos OS.

Description Restart the access point.

Options *name*—Restart a specific access point on the services gateway.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

request wlan access-point restart wap-3

```
user@host> request wlan access-point restart wap-3
Successfully restarted the access point.
```


Copyright © 2011, Juniper Networks, Inc.

CHAPTER 26

Restart Commands

This section contains the following topics:

- Restart Commands Overview on page 1133

Restart Commands Overview

Use the **restart** operational commands to restart software processes on the device. Operational commands are organized alphabetically.

Related Documentation

- *Junos OS CLI User Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

restart

Syntax

restart
<audit-process | chassis-control | class-of-service | **dhcp** | **dialer-services** |event-processing | firewall | **group-key-server** | interface-control | ipsec-key-management | **isdn-signaling** | l2ald | l2-learning | mib-process | pgm | ppp | pppoe | remote-operations | routing <logical-system *logical-system-name*> | sampling | service-deployment | snmp | **usb-control** | **wan-acceleration** | **web-management**>
<gracefully | immediately | soft>

Release Information

Command introduced before Release 7.4 of Junos OS.
wan-acceleration option added in Release 8.5 of Junos OS.
group-key-server option added in Release 10.2 of Junos OS.

Description

Restart a Junos OS process.

CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

Options

dhcp—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.

dialer-services—(Optional) Restart the ISDN dial out process.

group-key-server—(Optional) Restart the group VPN server process. The group VPN server loses all its data, including TEK and KEK keys, when it restarts. New keys are generated, but the keys are not available to group members until they reregister.

isdn-signaling—(Optional) Restart the ISDN signaling process, which initiates ISDN connections.

usb-control—(Optional) Restart the USB control process.

wan-acceleration—(J Series devices only.) (Optional) Restart the WAN acceleration process. If the WXC Integrated Services Module (ISM 200) is not accessible, or is not responding, you can use this command to restart the WAN acceleration process.

web-management—(Optional) Restart the Web management process.

Required Privilege Level

reset

List of Sample Output

restart interfaces on page 1134

Output Fields

When you enter this command, you are provided feedback on the status of your request.

restart interfaces

`user@host>` **restart interfaces**

Copyright © 2011, Juniper Networks, Inc.

```
interfaces process terminated
interfaces process restarted
```

Copyright © 2011, Juniper Networks, Inc.

CHAPTER 27

Show Commands

This section contains the following topics:

- Show Commands Overview on page 1137

Show Commands Overview

Use the **show** operational commands to review and verify the validity of your configurations and monitor device operation. Operational commands are organized alphabetically.

Related Documentation

- *Junos OS Interfaces Command Reference*
- *Junos OS Routing Protocols and Policies Command Reference*
- *Junos OS System Basics and Services Command Reference*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2011, Juniper Networks, Inc.

show bgp neighbor

Syntax

show bgp neighbor
< *neighbor-address*>
<**instance** *instance* >

Release Information

Command modified in Release 8.5 of Junos OS.

Description

Display the state of the specified Border Gateway Protocol (BGP) neighbor. If a peer is forced to Idle state because of license check failure, the output displays the state and the reason—**LicenseCheckFailed**.

Options

instance ***instance***—(Optional) Display peer information for a particular routing instance.

neighbor-address—(Optional) Display information for only the BGP peer at the specified IP address.

Required Privilege Level

view

Related Documentation

- *Junos OS Routing Protocols and Policies Command Reference*

List of Sample Output

show bgp neighbor 5.5.5.2 on page 1140
show bgp neighbor instance master on page 1140

Output Fields

Table 7 on page 1138 lists the output fields for the **show bgp neighbor** command. Output fields are listed in the approximate order in which they appear.

Table 7: show bgp neighbor Output Fields

Field Name	Field Description
Peer	Address of the BGP neighbor. The address is followed by the neighbor's port number.
AS	AS number of the peer.
Local	Address of the local device. The address is followed by the peer's port number.
Type	Type of peer: Internal or External.
State	Current state of the BGP session: • **Active**—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. • **Connect**—BGP is waiting for the transport protocol connection to complete. • **Established**—The BGP session has been established, and the peers are exchanging update messages. • **Idle**—Either the BGP license check failed, or this is the first stage of a connection and BGP is waiting for a Start event. • **OpenConfirm**—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. • **OpenSent**—BGP has sent an open message and is waiting to receive an open message from the peer.

Copyright © 2011, Juniper Networks, Inc.

Table 7: show bgp neighbor Output Fields *(continued)*

Field Name	Field Description
Flags	Internal BGP flags: • **Aggregate Label**—BGP has aggregated a set of incoming labels (labels received from the peer) into a single forwarding label. • **CleanUp**—The peer session is being shut down. • **Delete**—This peer has been deleted. • **Idled**—This peer has been permanently idled. • **Initializing**—The peer session is initializing. • **SendRtn**—Messages are being sent to the peer. • **Sync**—This peer is synchronized with the rest of the peer group. • **TryConnect**—Another attempt is being made to connect to the peer. • **Unconfigured**—This peer is not configured. • **WriteFailed**—An attempt to write to this peer failed. • **Last State**—Previous state of the BGP session.
Last State	Previous state of the BGP session.
Last Event	Last activity that occurred in the BGP session: • **Closed**—The BGP session closed. • **ConnectRetry**—The transport protocol connection failed, and BGP is trying again to connect. • **HoldTime**—The session ended because the hold timer expired. • **KeepAlive**—The local device sent a BGP keepalive message to the peer. • **Open**—The local device sent a BGP open message to the peer. • **OpenFail**—The local device did not receive an acknowledgment of a BGP open message from the peer. • **RecvKeepAlive**—The local device received a BGP keepalive message from the peer. • **RecvNotify**—The local device received a BGP notification message from the peer. • **RecvOpen**—The local device received a BGP open message from the peer. • **RecvUpdate**—The local device received a BGP update message from the peer. • **Start**—The peering session started. • **Stop**—The peering session stopped. • **TransportError**—A TCP error occurred.
Last Error	Last error that occurred in the BGP session: • **Cease**—An error occurred, such as a version mismatch, that caused the session to close. • **Finite State Machine Error**—In setting up the session, BGP received a message that it did not understand. • **Hold Time Expired**—The session's hold time expired. • **Message Header Error**—The header of a BGP message was malformed. • **Open Message Error**—A BGP open message contained an error. • **None**—No errors occurred in the BGP session. • **Update Message Error**—A BGP update message contained an error.
Export	Name of the export policy that is configured on the peer.
Import	Name of the import policy that is configured on the peer.

Copyright © 2011, Juniper Networks, Inc.

Table 7: show bgp neighbor Output Fields *(continued)*

Field Name	Field Description
Options	Configured BGP options: • **AddressFamily**—Configured address family: inet or inet-vpn. • **GracefulRestart**—Graceful restart is configured. • **HoldTime**—Hold time configured with the **hold-time** statement. The hold time is three times the interval at which keepalive messages are sent. • **Local Address**—Address configured with the **local-address** statement. • **NLRI**—Configured multicast BGP state for the BGP group: multicast, unicast, or both if you have configured **nlri any**. • **Peer AS**—Configured peer autonomous system (AS). • **Preference**—Preference value configured with the **preference** statement. • **Refresh**—Configured to refresh automatically when the policy changes. • **Rib-group**—Configured routing table group.
Address families configured	Names of configured address families for the VPN.
Local Address	Address of the local device.
Holdtime	Hold time configured with the **hold-time** statement. The hold time is three times the interval at which keepalive messages are sent.
Preference	Preference value configured with the **preference** statement.
Number of flaps	Number of times the BGP session has gone down and then come back up.
Trace file	Name of the file to receive the output of the tracing operation.

show bgp neighbor 5.5.5.2

```
user@host> show bgp neighbor 5.5.5.2
  Type: Internal    State: Idle (LicenseCheckFailed)   Flags: <ImportEval Sync>
Peer: 5.5.5.2 AS 200           Local: unspecified AS 200
  Type: Internal    State: Idle (LIcenseCheckFailed)       (route reflector
client)Flags: <ImportEval>
  Last State: Idle          Last Event: Start
  Last Error: None
  Options: <Preference LogUpDown Cluster AddressFamily PeerAS Rib-group Refresh>

  Address families configured: inet-unicast inet-vpn-unicast l2vpn-signaling
  Holdtime: 90 Preference: 170
  Number of flaps: 0
  Trace options:  all
  Trace file: /var/log/bgp size 131072 files 10
```

show bgp neighbor instance master

```
user@host> show bgp neighbor instance master
Peer: 5.5.5.1 AS 200           Local: 5.5.5.2 AS 200
  Type: Internal    State: Idle (LicenseCheckFailed)         Flags: <>
  Last State: Idle          Last Event: Start
  Last Error: Cease
  Export: [ static ]
  Options: <Preference LocalAddress LogUpDown AddressFamily PeerAS Rib-group
```


Copyright © 2011, Juniper Networks, Inc.

```
Refresh>
  Address families configured: inet-unicast inet-vpn-unicast
  Local Address: 5.5.5.2 Holdtime: 90 Preference: 170
  Number of flaps: 4
  Last flap event: RecvUpdate
  Error: 'Update Message Error' Sent: 3 Recv: 0
  Error: 'Cease' Sent: 2 Recv: 0
  Trace file: /var/log/bgp size 131072 files 10
```

show configuration smtp

Syntax show configuration smtp

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display complete SMTP information.

Options apply-groups—Groups from which SMTP inherits configuration data.

apply-groups-except—Groups from which SMTP restricts inheriting configuration data.

Required Privilege Level view

List of Sample Output **show smtp configuration on page 1142**

Output Fields Table 8 on page 1142 describes the output fields for the **show smtp configuration** command.

Table 8: show smtp configuration

Field Name	Field Description	Level of Output
address	SMTP server's IPv4 address	All levels
login	Configure a mail sender account to the server	All levels
password	Default sender password for user authentication	All levels

show smtp configuration

```
user@host> show smtp configuration
primary-server {
    address 218.102.48.213;
    login "dayone@netvigator.com" {
        password "$9$YhgoZ.PQ6CuTQ1KMLN-qmP"; ## SECRET-DATA
    }
}
```


Copyright © 2011, Juniper Networks, Inc.

show chassis cluster control-plane statistics

Syntax **show chassis cluster control-plane statistics**

Release Information Command introduced in Release 9.3 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

Description Display information about chassis cluster control plane statistics.

Required Privilege Level view

Related Documentation
- **clear chassis cluster control-plane statistics on page 1002**

List of Sample Output **show chassis cluster control-plane statistics on page 1143**
show chassis cluster control-plane statistics (SRX3000 and SRX5000 line devices) on page 1144

Output Fields Table 9 on page 1143 lists the output fields for the **show chassis cluster control-plane statistics** command. Output fields are listed in the approximate order in which they appear.

Table 9: show chassis cluster control-plane statistics Output Fields

Field Name	Field Description
Control link statistics	Statistics of the control link used by chassis cluster traffic. Statistics for **Control link 1** are displayed when you use dual control links (SRX3000 and SRX5000 lines only). • **Heartbeat packets sent**—Number of heartbeat messages sent on the control link. • **Heartbeat packets received**—Number of heartbeat messages received on the control link. • **Heartbeat packet errors**—Number of heartbeat errors received on the control link
Fabric link statistics	Statistics of the fabric link used by chassis cluster traffic. • **Probes sent**—Number of probes sent. • **Probes received**—Number of probes received. • **Probe errors**—Number of probe errors received.
Switch fabric link statistics	Statistics of the switch fabric link used by chassis cluster traffic. • **Probe state**—State of the probe, **UP** or **DOWN**. • **Probes sent**—Number of probes sent. • **Probes received**—Number of probes received. • **Probe recv error** —Error in receiving probe. • **Probe send error**—Error in sending probe.

show chassis cluster control-plane statistics

```
user@host> show chassis cluster control-plane statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 11646
        Heartbeat packets received: 8343
```

```
        Heartbeat packet errors: 0
Fabric link statistics:
    Probes sent: 11644
    Probes received: 8266
    Probe errors: 0

Switch fabric link statistics:
    Probe state : DOWN
    Probes sent: 8145
    Probes received: 8013
    Probe recv errors: 0
    Probe send errors: 0
```

show chassis cluster control-plane statistics (SRX3000 and SRX5000 line devices)

```
user@host> show chassis cluster control-plane statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 258698
        Heartbeat packets received: 258693
    Control link 1:
        Heartbeat packets sent: 258698
        Heartbeat packets received: 258693
Fabric link statistics:
    Probes sent: 258690
    Probes received: 258690
```


Copyright © 2011, Juniper Networks, Inc.

show chassis cluster data-plane interfaces

Syntax **show chassis cluster data-plane interfaces**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the status of the data plane interface (also known as a fabric interface) in a chassis cluster configuration.

Required Privilege Level view

List of Sample Output **show chassis cluster data-plane interfaces on page 1145**

Output Fields Table 10 on page 1145 lists the output fields for the **show chassis cluster data-plane interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 10: show chassis cluster data-plane interfaces Output Fields

Field Name	Field Description
fab0/fab1	Name of the logical fabric interface. • **Name**—Name of the physical Ethernet interface. • **Status**—State of the fabric interface: **up** or **down**.

show chassis cluster data-plane interfaces

```
user@host> show chassis cluster data-plane interfaces
fab0:
    Name                Status
    ge-2/1/9            up
    ge-2/2/5            up
fab1:
    Name                Status
    ge-8/1/9            up
    ge-8/2/5            up
```

show chassis cluster data-plane statistics

Syntax **show chassis cluster data-plane statistics**

Release Information Command introduced in Release 9.3 of Junos OS.

Description Display information about chassis cluster data plane statistics.

Required Privilege Level view

Related Documentation
- **clear chassis cluster data-plane statistics on page 1003**

List of Sample Output **show chassis cluster data-plane statistics on page 1147**

Output Fields Table 11 on page 1146 lists the output fields for the **show chassis cluster data-plane statistics** command. Output fields are listed in the approximate order in which they appear.

Table 11: show chassis cluster data-plane statistics Output Fields

Field Name	Field Description
Services Synchronized	• **Service name**—Name of the service. • **Rtos sent**—Number of runtime objects (RTOs) sent. • **Rtos received**—Number of RTOs received. • **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context. • **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service. • **Resource manager**—Messages synchronizing resource manager groups and resources. • **Session create**—Messages synchronizing session creation. • **Session close**—Messages synchronizing session close. • **Session change**—Messages synchronizing session change. • **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall). • **Session ageout refresh request**—Messages synchronizing request session after ageout. • **Session ageout refresh reply**—Messages synchronizing reply session after ageout. • **IPsec VPN**—Messages synchronizing VPN session. • **Firewall user authentication**—Messages synchronizing firewall user authentication session. • **MGCP ALG**—Messages synchronizing MGCP ALG sessions. • **H323 ALG**—Messages synchronizing H.323 ALG sessions. • **SIP ALG**—Messages synchronizing SIP ALG sessions. • **SCCP ALG**—Messages synchronizing SCCP ALG sessions. • **PPTP ALG**—Messages synchronizing PPTP ALG sessions. • **RTSP ALG**—Messages synchronizing RTSP ALG sessions.

Copyright © 2011, Juniper Networks, Inc.

show chassis cluster data-plane statistics

```
user@host> show chassis cluster data-plane statistics
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              0            0
    Session close                               0            0
    Session change                              0            0
    Gate create                                 0            0
    Session ageout refresh requests             0            0
    Session ageout refresh replies              0            0
    IPsec VPN                                   0            0
    Firewall user authentication                0            0
    MGCP ALG                                    0            0
    H323 ALG                                    0            0
    SIP ALG                                     0            0
    SCCP ALG                                    0            0
    PPTP ALG                                    0            0
    RTSP ALG                                    0            0
```

show chassis cluster interfaces

Syntax **show chassis cluster interfaces**

Release Information Command modified in Release 9.0 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

Description Display the status of the control interface in a chassis cluster configuration.

Required Privilege Level view

List of Sample Output **show chassis cluster interfaces on page 1148**
show chassis cluster interfaces (SRX3000 and SRX5000 line devices) on page 1148

Output Fields Table 12 on page 1148 lists the output fields for the **show chassis cluster interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 12: show chassis cluster interfaces Output Fields

Field Name	Field Description
Control link 0 name **Control link 1 name**	Name and status of the chassis cluster control interface. **Control link 1 name** is displayed when you use dual control links (SRX3000 and SRX5000 lines only).
Redundant-ethernet Information	• **Name**—Name of the redundant Ethernet interface. • **Status**—State of the interface: **up** or **down**. • **Redundancy-group**—ID number (1-255) of the redundancy group associated with the redundant Ethernet interface.
Interface Monitoring	• **Interface**—Name of the interface to be monitored. • **Weight**—Relative importance of the interface to redundancy group operation. • **Status**—State of the interface: **up** or **down**. • **Redundancy-group**—Identification number of the redundancy group associated with the interface.

show chassis cluster interfaces

```
user@host> show chassis cluster interfaces
Control link 0 name: em0
Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
Interface Monitoring:
    Interface         Weight    Status    Redundancy-group
    ge-6/0/0          200       Up        1
```

show chassis cluster interfaces (SRX3000 and SRX5000 line devices)

```
user@host> show chassis cluster interfaces
Control link 0 name: em0
Control link 1 name: em1
Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
Interface Monitoring:
```

 Copyright © 2011, Juniper Networks, Inc.

```
Interface          Weight    Status    Redundancy-group
ge-6/0/0           200       Up        1
```

show chassis cluster ip-monitoring status redundancy-group

Syntax **show chassis cluster ip-monitoring status <redundancy-group *group-number* >**

Release Information Command added in Release 9.6 of Junos OS.

Description Display the status of all monitored IP addresses for a redundancy group.

Options none— Display the status of monitored IP addresses for all redundancy groups on the node.

redundancy-group *group-number* — Display the status of monitored IP addresses under the specified redundancy group.

Required Privilege Level view

Related Documentation

- **redundancy-group on page 96**
- **clear chassis cluster failover-count on page 1004**
- **request chassis cluster failover node on page 1095**
- **request chassis cluster failover reset on page 1096**

List of Sample Output **show chassis cluster ip-monitoring status on page 1151**
show chassis cluster ip-monitoring status redundancy-group on page 1151

Output Fields Table 13 on page 1150 lists the output fields for the **show chassis cluster ip-monitoring status** command.

Table 13: show chassis cluster ip-monitoring status Output Fields

Field Name	Field Description
Redundancy-group	ID number (0 - 255) of a redundancy group in the cluster.
IP Address	Monitored IP address in the redundancy group.
Status	Current reachability state of the monitored IP address. Values for this field are: **reachable**, **unreachable**, and **unknown**. The status is “unknown” if packet forwarding engines (PFEs) are not yet up and running.
Failure count	Number of attempts to reach an IP address.
Reason	Explanation for the reported status. See Table 14 on page 1151.

Expanded reason output fields for unreachable IP addresses added in Release 10.1 of Junos OS. You might see any of the following reasons displayed.

 Copyright © 2011, Juniper Networks, Inc.

Table 14: show chassis cluster ip-monitoring status redundancy group Reason Fields

Reason	Reason Description
No route to host	The router could not resolve the ARP, which is needed to send the ICMP packet to the host with the monitored IP address.
No auxiliary IP found	The redundant Ethernet interface does not have an auxiliary IP address configured.
Reth child not up	A child interface of a redundant Ethernet interface is down.
redundancy-group state unknown	Unable to obtain the state (primary, secondary, secondary-hold, disable) of a redundancy-group.
No reth child MAC address	Could not extract the MAC address of the redundant Ethernet child interface.
Secondary link not monitored	The secondary link may be down (the secondary child interface of a redundant Ethernet interface is either down or non-functional).
Unknown	The IP address has just been configured and the router still does not know the status of this IP. or Do not know the exact reason for the failure.

show chassis cluster ip-monitoring status

```
user@host> show chassis cluster ip-monitoring status
node0:
--------------------------------------------------------------------------

Redundancy group: 1

IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a

node1:
--------------------------------------------------------------------------

Redundancy group: 1

IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a
```

show chassis cluster ip-monitoring status redundancy-group

```
user@host> show chassis cluster ip-monitoring status redundancy-group 1
node0:
--------------------------------------------------------------------------

Redundancy group: 1
```

```
IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a

node1:
--------------------------------------------------------------------------

Redundancy group: 1

IP address                Status        Failure count  Reason
10.254.5.44               reachable       0            n/a
2.2.2.1                   reachable       0            n/a
1.1.1.5                   reachable       0            n/a
1.1.1.4                   reachable       0            n/a
1.1.1.1                   reachable       0            n/a
```


Copyright © 2011, Juniper Networks, Inc.

show chassis cluster statistics

Syntax **show chassis cluster statistics**

Release Information Command modified in Release 9.0 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

Description Display information about chassis cluster services and interfaces.

Required Privilege Level view

Related Documentation
- **clear chassis cluster statistics on page 1008**

List of Sample Output
show chassis cluster statistics on page 1154
show chassis cluster statistics (SRX3000 and SRX5000 line devices) on page 1155
show chassis cluster statistics (SRX3000 and SRX5000 line devices) on page 1155

Output Fields Table 15 on page 1153 lists the output fields for the **show chassis cluster statistics** command. Output fields are listed in the approximate order in which they appear.

Table 15: show chassis cluster statistics Output Fields

Field Name	Field Description
Control link statistics	Statistics of the control link used by chassis cluster traffic. Statistics for **Control link 1** are displayed when you use dual control links (SRX3000 and SRX5000 lines only). Note that the output for the SRX3000 and SRX5000 lines will always show **Control link 0** and **Control link 1** statistics, even though only one control link is active or working. • **Heartbeat packets sent**—Number of heartbeat messages sent on the control link. • **Heartbeat packets received**—Number of heartbeat messages received on the control link.
Fabric link statistics	Statistics of the fabric link used by chassis cluster traffic. • **Probes sent**—Number of probes sent. • **Probes received**—Number of probes received.

Table 15: show chassis cluster statistics Output Fields *(continued)*

Field Name	Field Description
Services Synchronized	• **Service name**—Name of the service. • **Rtos sent**—Number of runtime objects (RTOs) sent. • **Rtos received**—Number of RTOs received. • **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context. • **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service. • **Resource manager**—Messages synchronizing resource manager groups and resources. • **Session create**—Messages synchronizing session creation. • **Session close**—Messages synchronizing session close. • **Session change**—Messages synchronizing session change. • **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall). • **Session ageout refresh request**—Messages synchronizing request session after ageout. • **Session ageout refresh reply**—Messages synchronizing reply session after ageout. • **IPsec VPN**—Messages synchronizing VPN session. • **Firewall user authentication**—Messages synchronizing firewall user authentication session. • **MGCP ALG**—Messages synchronizing MGCP ALG sessions. • **H323 ALG**—Messages synchronizing H.323 ALG sessions. • **SIP ALG**—Messages synchronizing SIP ALG sessions. • **SCCP ALG**—Messages synchronizing SCCP ALG sessions. • **PPTP ALG**—Messages synchronizing PPTP ALG sessions. • **RTSP ALG**—Messages synchronizing RTSP ALG sessions. • **MAC address learning**—Messages synchronizing MAC address learning.

show chassis cluster statistics

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 798
        Heartbeat packets received: 784
Fabric link statistics:
    Probes sent: 793
    Probes received: 0
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              0            0
    Session close                               0            0
    Session change                              0            0
    Gate create                                 0            0
    Session ageout refresh requests             0            0
    Session ageout refresh replies              0            0
    IPsec VPN                                   0            0
    Firewall user authentication                0            0
    MGCP ALG                                    0            0
    H323 ALG                                    0            0
```


Copyright © 2011, Juniper Networks, Inc.

```
    SIP ALG                                     0           0
    SCCP ALG                                    0           0
    PPTP ALG                                    0           0
    RTSP ALG                                    0           0
    MAC address learning                        0           0
```

show chassis cluster statistics (SRX3000 and SRX5000 line devices)

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
    Control link 1:
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
Fabric link statistics:
    Probes sent: 258681
    Probes received: 258681
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              1            0
    Session close                               1            0
    Session change                              0            0
    Gate create                                 0            0
    Session ageout refresh requests             0            0
    Session ageout refresh replies              0            0
    IPSec VPN                                   0            0
    Firewall user authentication                0            0
    MGCP ALG                                    0            0
    H323 ALG                                    0            0
    SIP ALG                                     0            0
    SCCP ALG                                    0            0
    PPTP ALG                                    0            0
    RPC ALG                                     0            0
    RTSP ALG                                    0            0
    RAS ALG                                     0            0
    MAC address learning                        0            0
    GPRS GTP                                    0            0
```

show chassis cluster statistics (SRX3000 and SRX5000 line devices)

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 82371
        Heartbeat packets received: 82321
    Control link 1:
        Heartbeat packets sent: 0
        Heartbeat packets received: 0
Fabric link statistics:
    Probes sent: 258681
    Probes received: 258681
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              1            0
    Session close                               1            0
    Session change                              0            0
    Gate create                                 0            0
```

```
Session ageout refresh requests          0            0
Session ageout refresh replies           0            0
IPSec VPN                                0            0
Firewall user authentication             0            0
MGCP ALG                                 0            0
H323 ALG                                 0            0
SIP ALG                                  0            0
SCCP ALG                                 0            0
PPTP ALG                                 0            0
RPC ALG                                  0            0
RTSP ALG                                 0            0
RAS ALG                                  0            0
MAC address learning                     0            0
GPRS GTP                                 0            0
```


Copyright © 2011, Juniper Networks, Inc.

show chassis cluster status

Syntax

show chassis cluster status
<redundancy-group ***group-number*** **>**

Release Information

Command modified in Release 9.2 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

Description

Display the failover status of a chassis cluster.

Options

none—Display the status of all redundancy groups in the chassis cluster.

redundancy-group ***group-number*** —(Optional) Display the status of the specified redundancy group.

Required Privilege Level

view

Related Documentation

- **redundancy-group on page 96**
- **clear chassis cluster failover-count on page 1004**
- **request chassis cluster failover node on page 1095**
- **request chassis cluster failover reset on page 1096**

List of Sample Output

show chassis cluster status on page 1158
show chassis cluster status redundancy-group 2 on page 1158
show chassis cluster status on page 1158
show chassis cluster status on page 1158

Output Fields

Table 16 on page 1157 lists the output fields for the **show chassis cluster status** command. Output fields are listed in the approximate order in which they appear.

Table 16: show chassis cluster status Output Fields

Field Name	Field Description
Cluster ID	ID number (1-15) of a cluster.
Redundancy-Group	ID number (1-255) of a redundancy group in the chassis cluster.
Node name	Node (device) in the chassis cluster (**node0** or **node1**).
Priority	Assigned priority for the redundancy group on that node.

Copyright © 2011, Juniper Networks, Inc.

Table 16: show chassis cluster status Output Fields *(continued)*

Field Name	Field Description
Status	State of the redundancy group (**Primary**, **Secondary**, **Lost**, or **Unavailable**). • **Primary**—Redundancy group is active and passing traffic. • **Secondary**—Redundancy group is passive and not passing traffic. • **Lost**—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster and due to control link failure, one node cannot exchange heartbeats, or when the other node is rebooted. • **Unavailable**—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node, or if only one node is present in the cluster.
Preempt	• **Yes**: Mastership can be preempted based on priority. • **No**: Change in priority will not preempt the mastership.
Manual failover	• **Yes**: If the Mastership is set manually through the CLI with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command. This overrides **Priority** and **Preempt**. • **No**: Mastership is not set manually through the CLI.

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 3
   Node name               Priority    Status    Preempt  Manual failover
 Redundancy-group: 0, Failover count: 1
    node0                   254         primary   no       no
    node1                   2           secondary no       no
 Redundancy-group: 1, Failover count: 1
    node0                   254         primary   no       no
    node1                   1           secondary no       no
```

show chassis cluster status redundancy-group 2

```
user@host> show chassis cluster status redundancy-group 2
Cluster ID: 14
   Node name          Priority    Status    Preempt  Manual failover
 Redundancy-Group: 2, Failover count: 1
    node0              50          secondary no       no
    node1              100         primary   no       no
```

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 15
Node                  Priority          Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 5
    node0                   200         primary        no       no
    node1                   0           lost           n/a      n/a
Redundancy group: 1 , Failover count: 41
    node0                   101         primary        no       no
    node1                   0           lost           n/a      n/a
```

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 15
Node                  Priority          Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 5
    node0                   200         primary        no       no
    node1                   0           unavailable    n/a      n/a
```


Copyright © 2011, Juniper Networks, Inc.

```
Redundancy group: 1 , Failover count: 41
    node0                   101         primary        no       no
    node1                   0           unavailable    n/a      n/a
```

show chassis cluster ethernet-switching interfaces

Syntax show chassis cluster ethernet-switching interfaces

Release Information Command introduced in Release 11.1 of Junos OS.

Description Display the status of the switch fabric interfaces (swfab) in a chassis cluster.

Required Privilege Level view

List of Sample Output **show chassis cluster ethernet-switching interfaces on page 1160**

Output Fields Table 17 on page 1160 lists the output fields for the **show chassis cluster ethernet-switching interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 17: show chassis cluster ethernet-switching interfaces Output Fields

Field Name	Field Description
swfab0/swfab1	Name of the switch fabric interface. • Name—Name of the physical interface. • Status—State of the swfab interface: up or down.

show chassis cluster ethernet-switching interfaces

```
user@host> show chassis cluster ethernet-switching interfaces
swfab0:
    Name                Status
    ge-0/0/9            up
    ge-0/0/10           up
swfab1:
    Name                Status
    ge-5/0/9            up
    ge-5/0/10           up
```


Copyright © 2011, Juniper Networks, Inc.

show chassis cluster ethernet-switching status

Syntax show chassis cluster ethernet-switching status

Release Information Command introduced in Release 11.1 of Junos OS.

Description Display the Ethernet switching status of the chassis cluster.

Required Privilege Level view

List of Sample Output **show chassis cluster ethernet-switching status on page 1161**

Output Fields Table 18 on page 1161 lists the output fields for the **show chassis cluster ethernet-switching status** command. Output fields are listed in the approximate order in which they appear.

Table 18: show chassis cluster ethernet-switching status Output Fields

Field Name	Field Description
Cluster ID	ID number (1-15) of a cluster.
Redundancy-Group	ID number (1-255) of a redundancy group in the chassis cluster.
Node name	Node (device) in the chassis cluster (**node0** or **node1**).
Priority	Assigned priority for the redundancy group on that node.
Status	State of the redundancy group (**Primary**, **Secondary**, **Lost**, or **Unavailable**). • **Primary**—Redundancy group is active and passing traffic. • **Secondary**—Redundancy group is passive and not passing traffic. • **Lost**—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster and due to control link failure, one node cannot exchange heartbeats, or when the other node is rebooted. • **Unavailable**—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node, or if only one node is present in the cluster.
Preempt	• **Yes**: Mastership can be preempted based on priority. • **No**: Change in priority will not preempt mastership.
Manual failover	• **Yes**: If mastership is set manually through the CLI. • **No**: Mastership is not set manually through the CLI.

show chassis cluster ethernet-switching status

```
user@host> show chassis cluster ethernet-switching status
Cluster ID: 10
Node                  Priority          Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   1           primary        no       no
    node1                   0           lost           n/a      n/a
```

```
Switch fabric link statistics:
    Probe state : DOWN
    Probes sent: 8145
    Probes received: 8013
    Probe recv errors: 0
    Probe send errors: 0
```


Copyright © 2011, Juniper Networks, Inc.

show chassis fpc

Syntax

show chassis fpc
<**detail** < ***pim-slot*** >| <node (***node-id*** | local | primary)>> |
<node (***node-id*** | local | primary)> |
<**pic-status** < ***pim-slot*** >| <node (***node-id*** | local | primary)>>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display status information about the installed Physical Interface Modules (PIMs) and PIM slots in a single device chassis or in a chassis cluster configuration.

Options

none—Display brief information about the state of the installed PIMs and PIM slots.

detail—(Optional) Display detailed PIM status information.

pim-slot —(Optional) Display information about the PIM in this slot.

node—(Optional) For chassis cluster configurations, display status information for all PIMs or for the specified PIM on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

pic-status—(Optional) Display status information for all PIMs or for the PIM in the specified slot (see ***pim-slot***). The PIM slot number is reported as an FPC number, and the PIM number (always 0) is reported as a PIC number.

Required Privilege Level

view

Related Documentation

- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show chassis fpc on page 1164
show chassis fpc (SRX5600 and SRX5800 devices) on page 1164
show chassis fpc detail on page 1165
show chassis fpc pic-status on page 1165
show chassis fpc pic-status (SRX5600 and SRX5800 devices) on page 1165

Output Fields

Table 19 on page 1164 lists the output fields for the **show chassis fpc** command. Output fields are listed in the approximate order in which they appear.

Table 19: show chassis fpc Output Fields

Field Name	Field Description
Slot or Slot State	Slot number and state. The state can be one of the following conditions: • **Dead**—Held in reset because of errors. • **Diag**—Slot is being ignored while the device is running diagnostics. • **Dormant**—Held in reset. • **Empty**—No PIM is present. • **Online**—PIM is online and running. • **Present**—PIM is detected by the device, but is either not supported by the current version of Junos OS or inserted in the wrong slot. The output also states either **Hardware Not Supported** or **Hardware Not In Right Slot**. PIM is coming up but not yet online. • **Probed**—Probe is complete; awaiting restart of the Packet Forwarding Engine (PFE). • **Probe-wait**—Waiting to be probed.
Temp (C) or Temperature	Temperature of the air passing by the PIM, in degrees Celsius or in both Celsius and Fahrenheit.
Total CPU Utilization (%)	Total percentage of CPU being used by the PIM's processor.
Interrupt CPU Utilization (%)	Of the total CPU being used by the PIM's processor, the percentage being used for interrupts.
Memory DRAM (MB)	Total DRAM, in megabytes, available to the PIM's processor.
Heap Utilization (%)	Percentage of heap space (dynamic memory) being used by the PIM's processor. If this number exceeds 80 percent, there may be a software problem (memory leak).
Buffer Utilization (%)	Percentage of buffer space being used by the PIM's processor for buffering internal messages.
Start Time	Time when the Routing Engine detected that the PIM was running.
Uptime	How long the Routing Engine has been connected to the PIM and, therefore, how long the PIM has been up and running.
PIC type	(**pic-status** output only) Type of PIM.

show chassis fpc

```
user@host> show chassis fpc
Temp  CPU Utilization (%)   Memory    Utilization (%)
    Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
      0  Online          -------------------- CPU less FPC --------------------
      1  Online          ---------------------  Not Usable --------------------
      2  Online          -------------------- CPU less FPC --------------------
```

show chassis fpc (SRX5600 and SRX5800 devices)

```
user@host> show chassis fpc
                      Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State             (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Empty
  1  Empty
  2  Empty
```


Copyright © 2011, Juniper Networks, Inc.

```
  3  Online            37      3          0       1024        7         42
  4  Empty
  5  Empty
  6  Online            30      8          0       1024       23         30
  7  Empty
  8  Empty
  9  Empty
 10  Empty
 11  Empty
```

show chassis fpc detail

```
user@host> show chassis fpc detail
 Slot 2 information:
      State                                Online
      Total CPU DRAM                       ---- CPU less FPC ----
      Start time                           2002-01-07 17:11:28 PST
      Uptime                               2 days, 8 hours, 38 minutes, 5 seconds
```

show chassis fpc pic-status

```
user@host> show chassis fpc pic-status
node0:
--------------------------------------------------------------------------
Slot 0   Online       FPC
  PIC 0  Online       4x GE Base PIC
Slot 3   Online       FPC
  PIC 0  Online       4x FE
Slot 6   Online       FPC
  PIC 0  Online       8x GE uPIM
node1:
--------------------------------------------------------------------------
Slot 0   Offline      FPC
Slot 3   Offline      FPC
Slot 6   Offline      FPC
```

show chassis fpc pic-status (SRX5600 and SRX5800 devices)

```
user@host> show chassis fpc pic-status
Slot 3   Online       SRX5k SPC
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
Slot 6   Online       SRX5k DPC 4x 10GE
  PIC 0  Online       1x 10GE(LAN/WAN) RichQ
  PIC 1  Online       1x 10GE(LAN/WAN) RichQ
  PIC 2  Online       1x 10GE(LAN/WAN) RichQ
  PIC 3  Online       1x 10GE(LAN/WAN) RichQ
```

show chassis hardware

Syntax

show chassis hardware
<**clei-models** | **detail** | **extensive** | models | node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display chassis hardware information.

Options

clei-models—(Optional) Display Common Language Equipment Identifier Code (CLEI) barcode and model number for orderable field-replaceable units (FRUs).

detail | **extensive**—(Optional) Display the specified level of output.

models—(Optional) Display model numbers and part numbers for orderable FRUs.

node—(Optional) For chassis cluster configurations, display chassis hardware information on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show chassis hardware on page 1168
show chassis hardware (SRX5600 and SRX5800 devices) on page 1168
show chassis hardware detail on page 1168
show chassis hardware detail node 1 on page 1168
show chassis hardware extensive on page 1169
show chassis hardware models (SRX5600 and SRX5800 devices) on page 1170
show chassis hardware clei-models (SRX5600 and SRX5800 devices) on page 1170

Output Fields

Table 20 on page 1166 lists the output fields for the **show chassis hardware** command. Output fields are listed in the approximate order in which they appear.

Table 20: show chassis hardware Output Fields

Field Name	Field Description
Item	Chassis component—Information about the backplane; power supplies; fan trays; Routing Engine; each Physical Interface Module (PIM)—reported as FPC and PIC—and each fan, blower, and impeller.
Version	Revision level of the chassis component.

Copyright © 2011, Juniper Networks, Inc.

Table 20: show chassis hardware Output Fields *(continued)*

Field Name	Field Description
Part Number	Part number for the chassis component.
Serial Number	Serial number of the chassis component. The serial number of the backplane is also the serial number of the device chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the device chassis.
Assb ID or Assembly ID	Identification number that describes the FRU hardware.
FRU model number	Model number of FRU hardware component.
CLEI code	Common Language Equipment Identifier code. This value is displayed only for hardware components that use ID EEPROM format v2. This value is not displayed for components that use ID EEPROM format v1.
EEPROM Version	ID EEPROM version used by hardware component: 0x01 (version 1) or 0x02 (version 2).

Description	Brief description of the hardware item:
	• Type of power supply.
	• Type of PIM. If the PIM type is not supported on the current software release, the output states **Hardware Not Supported**.
	• Type of FPC: The FPC type corresponds to the PIM. The following shows the PIM abbreviation in the output and the corresponding PIM name:
	  ◦ 2x FE—Dual-Port Fast Ethernet PIM
	  ◦ 4x FE—4-Port Fast Ethernet ePIM
	  ◦ 1x GE Copper—Copper Gigabit Ethernet ePIM (one 10-mpbs, 100-Mpbs, or 1000-Mpbs port)
	  ◦ 1x GE SFP—SFP Gigabit Ethernet ePIM (one fiber port)
	  ◦ 1x SFP uPIM—1-Port Gigabit Ethernet uPIM
	  ◦ 6x GE SFP uPIM—6-Port Gigabit Ethernet uPIM
	  ◦ 8x GE SFP uPIM—8-Port Gigabit Ethernet uPIM
	  ◦ 16x GE SFP uPIM—16-Port Gigabit Ethernet uPIM
	  ◦ 4x GE Base PIC—Four built-in Gigabit Ethernet ports on a chassis (fixed PIM)
	  ◦ 2x Serial—Dual-Port Serial PIM
	  ◦ 2x T1—Dual-Port T1 PIM
	  ◦ 2x E1—Dual-Port E1 PIM
	  ◦ 2x CT1E1/PRI—Dual-Port Channelized T1/E1/ISDN PRI PIM
	  ◦ 1x T3—T3 PIM (one port)
	  ◦ 1x E3—E3 PIM (one port)
	  ◦ 4x BRI S/T—4-Port ISDN BRI S/T PIM
	  ◦ 4x BRI U—4-Port ISDN BRI U PIM
	  ◦ 1x ADSL Annex A—ADSL 2/2 + Annex A PIM (one port, for POTS)
	  ◦ 1x ADSL Annex B—ADSL 2/2 + Annex B PIM (one port, for ISDN
	  ◦ 2x SHDSL (ATM)—G.SHDSL PIM (2-port two-wire mode or 1-port four-wire mode)
	  ◦ Integrated Services Module—WXC Integrated Services Module (ISM 200)
	• For hosts, the Routing Engine type.

Copyright © 2011, Juniper Networks, Inc.

show chassis hardware

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN001340AA        JSR2300
Routing Engine   REV 07   750-009992   AA04350184        RE-J.1
FPC 0            REV 04   750-010738   AB04330259        FPC
  PIC 0                                                  2x FE, 2x T1
Power Supply 0
```

show chassis hardware (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN10B7005AGA      SRX 5800
Midplane         REV 03   710-013698   TR0779            SRX 5800 Backplane
FPM Board        REV 03   710-014974   KC3406            Front Panel Display
PDM             Rev 03   740-013110   QCS1122504F      Power Distribution Module
PEM 1            Rev 03   740-013683   QCS1134703V       DC Power Entry Module
PEM 2            Rev 03   740-013683   QCS1134700E       DC Power Entry Module
Routing Engine 0 REV 06   740-015113   1000696955        RE-S-1300
CB 0             REV 07   710-013385   JZ3257            SRX5k SCB
FPC 3            BB-P2-39 710-020305   JS4847            SRX5k SPC
  CPU            REV 06   710-013713   KC1180            DPC PMB
  PIC 0                   BUILTIN      BUILTIN           SPU Cp
  PIC 1                   BUILTIN      BUILTIN           SPU Flow
FPC 6            REV 03   750-020751   JT0109            SRX5k DPC 4x 10GE
  CPU            REV 06   710-013713   KC3543            DPC PMB
  PIC 0                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
    Xcvr 0                NON-JNPR     A7C00SY           XFP-10G-SR
  PIC 1                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
    Xcvr 0       REV 01   740-011571   C728XJ01W         XFP-10G-SR
  PIC 2                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
  PIC 3                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
Fan Tray 0       REV 04   740-014971   TP1432            Fan Tray
Fan Tray 1       REV 04   740-014971   TP1829            Fan Tray
```

show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
    Chassis                                JN000968AB        J4300
    Midplane         REV 05   710-010001   ad04420077
    System IO        REV 07   710-010003   AE04420393        System IO board
    Routing Engine   REV 08   750-010005   btrd43500196      RE-J.2
      ad0     488 MB  512MB CHH            504754C53A711400  Compact Flash
      ad2     488 MB  512MB CHH            504754C43A711400  Removable Compact
Flash
    FPC 2            REV 08   750-013493   NB9161            FPC
      PIC 0                                                  Integrated Services
 Module
      ANNEX          REV 08   750-013493   NB9161            Integrated Services
```

show chassis hardware detail node 1

```
user@host> show chassis hardware detail node 1
node1:
--------------------------------------------------------------------------
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN108C688ADB      J6350
Midplane         REV 03   710-014593   NM7516
System IO        REV 01   710-016210   NN9781            JX350 System IO
Crypto Module                                            Crypto Acceleration
Routing Engine   REV 08   710-015273   NM6569            RE-J6350-3400
```


Copyright © 2011, Juniper Networks, Inc.

```
  ad0     991 MB  1GB CKS              20060000000000000800 Compact Flash
FPC 0                                                        FPC
FPC 3            REV 06   750-013492   NM1294               FPC
FPC 6            REV 11   750-015153   NP8750               FPC
```

show chassis hardware extensive

```
user@host> show chassis hardware extensive
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN107a494ADA      J4350
 Jedec Code:   0x0000            EEPROM Version:    0x00
 P/N:          ...........       S/N:               JN107a494ADA
 Assembly ID:  0x0513            Assembly Version:  00.00
 Date:         00-00-0000        Assembly Flags:    0x00
 Version:      ...........
 ID: j4350
...
FPC 5            REV 08   750-013493   NB9161               FPC
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 P/N:          750-013493        S/N:               S/N NB9161
 Assembly ID:  0x073c            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 Version:      REV 08
 ID: FPC                         FRU Model Number:  SSG-EPIM-1TX
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 01 ff 07 3c 01 08 52 45 56 20 30 38 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 31 33 34 39 33 00 00
  Address 0x20: 53 2f 4e 20 4e 42 39 31 36 31 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
  PIC 0                                                      Integrated Services
Module
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 Assembly ID:  0x063c            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 ID: Integrated Services Module
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 01 ff 06 3c 01 08 00 00 00 00 00 00 00 00
  Address 0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  Address 0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ed c0 0e 0b 00 00 00 00 00 00 00 00
  ANNEX          REV 08   750-013493   NB9161               Integrated Services
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 P/N:          750-013493        S/N:               S/N NB9161
 Assembly ID:  0x0808            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 Version:      REV 08
 ID: Integrated Services         FRU Model Number:  SSG-EPIM-1TX
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
```

```
  Address 0x00: 7f b0 01 ff 08 08 01 08 52 45 56 20 30 38 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 31 33 34 39 33 00 00
  Address 0x20: 53 2f 4e 20 4e 42 39 31 36 31 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

show chassis hardware models (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware models
Hardware inventory:
Item             Version  Part number  Serial number     FRU model number
Midplane         REV 03   710-013698   TR0779            CHAS-BP-MX960-S
FPM Board        REV 03   710-014974   KC3406            CRAFT-MX960-S
Routing Engine 0 REV 06   740-015113   1000696955        RE-S-1300-2048-S
CB 0             REV 07   710-013385   JZ3257            SCB-MX960-S
```

show chassis hardware clei-models (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware clei-models
Hardware inventory:
Item             Version  Part number  CLEI code         FRU model number
FPM Board        REV 02   710-017254                     CRAFT-MX480-S
Routing Engine 0 REV 06   740-015113                     RE-S-1300-2048-S
CB 0             REV 07   710-013385                     SCB-MX960-S
Fan Tray                                                 SRX5600-FAN
```


Copyright © 2011, Juniper Networks, Inc.

show dhcpv6 server binding

Syntax

show dhcpv6 server binding
<brief | detail | summary>
<interface *interface-name*>
<routing-instance *routing-instance-name*>

Release Information

Command introduced in Release 10.4 of Junos OS.

Description

Display the address bindings in the client table for DCHPv6 local server.

Options

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcpv6 server binding**.

interface *interface-name*—(Optional) Display information about active client bindings on the specified interface.

routing-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege Level

view

Related Documentation

- **clear dhcpv6 server binding on page 1009**

List of Sample Output

show dhcpv6 server binding on page 1172
show dhcpv6 server binding detail on page 1173
show dhcpv6 server binding interface on page 1173
show dhcpv6 server binding interface detail on page 1173
show dhcpv6 server binding prefix on page 1174
show dhcpv6 server binding session-id on page 1174
show dhcpv6 server binding summary on page 1174

Output Fields

Table 21 on page 1171 lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 21: show dhcv6p server binding Output Fields

Field Name	Field Description	Level of Output
number clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* releasing)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Prefix	Client's DHCPv6 prefix.	brief detail

Table 21: show dhcv6p server binding Output Fields *(continued)*

Field Name	Field Description	Level of Output
Session Id	Session ID of the subscriber session.	**brief** **detail**
Expires	Number of seconds in which lease expires.	**brief** **detail**
State	State of the address binding table on the DHCPv6 local server: • **BOUND**—Client has active IP address lease. • **INIT**—Initial state. • **RELEASE**—Client is releasing IP address lease. • **RECONFIGURE**—Client has received reconfigure message from server. • **RENEWING**—Client sending request to renew IP address lease. • **REQUESTING**—Client requesting a DHCPv6 server. • **SELECTING**—Client receiving offers from DHCPv6 servers.	**brief** **detail**
Interface	Interface on which the DHCPv6 request was received.	**brief**
Client DUID	Client's DHCP Unique Identifier (DUID).	**brief** **detail**
Lease expires	Date and time at which the client's IP address lease expires.	**detail**
Lease expires in	Number of seconds in which lease expires.	**detail**
Lease Start	Date and time at which the client's address lease was obtained.	**detail**
Incoming Client Interface	Client's incoming interface.	**detail**
Server IP Address	IP address of DHCPv6 server.	**detail**
Server Interface	Interface of DHCPv6 server.	**detail**
Client Id length	Length of the DHCPv6 client ID, in bytes.	**detail**
Client Id	ID of the DHCPv6 client.	**detail**

show dhcpv6 server binding

```
user@host> show dhcpv6 server binding

Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
```


Copyright © 2011, Juniper Networks, Inc.

```
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
Session Id:  6
     Client IPv6 Prefix:                    2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

     State:                                 BOUND(bound)
     Lease Expires:                         2009-07-21 10:41:15 PDT
     Lease Expires in:                      86308 seconds
     Lease Start:                           2009-07-20 10:41:15 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Ip Address:                     0.0.0.0
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001

Session Id:  7
     Client IPv6 Prefix:                    2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                 BOUND(bound)
     Lease Expires:                         2009-07-21 10:41:15 PDT
     Lease Expires in:                      86308 seconds
     Lease Start:                           2009-07-20 10:41:15 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Ip Address:                     0.0.0.0
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding interface

```
user@host> show dhcp6 server binding interface ge-1/0/0:10-101
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 1           86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01
```

show dhcpv6 server binding interface detail

```
user@host> show dhcp6 server binding interface ge-1/0/0:10-101 detail
Session Id:  7
     Client IPv6 Prefix:                    2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                 BOUND(bound)
     Lease Expires:                         2009-07-21 10:41:15 PDT
     Lease Expires in:                      86136 seconds
     Lease Start:                           2009-07-20 10:41:15 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Ip Address:                     0.0.0.0
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding prefix

```
user@host> show dhcp6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id:  7
     Client IPv6 Prefix:                    2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                 BOUND(bound)
     Lease Expires:                         2009-07-21 10:41:15 PDT
     Lease Expires in:                      86136 seconds
     Lease Start:                           2009-07-20 10:41:15 PDT
     Incoming Client Interface:             ge-1/0/0.0
     Server Ip Address:                     0.0.0.0
     Server Interface:                      none
     Client Id Length:                      14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding session-id

```
user@host> show dhcpv6 server binding 8
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 8           86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```


Copyright © 2011, Juniper Networks, Inc.

show dhcpv6 server statistics

Syntax **show dhcpv6 server statistics**
<routing-instance *routing-instance-name*>

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display DHCPv6 local server statistics.

Options routing-instance *routing-instance-name*—(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level view

Related Documentation
- **clear dhcpv6 server statistics on page 1010**

List of Sample Output **show dhcpv6 server statistics on page 1176**

Output Fields Table 22 on page 1175 lists the output fields for the **show dhcpv6 server statistics** command. Output fields are listed in the approximate order in which they appear.

Table 22: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. • **Total**—Total number of packets discarded by the DHCPv6 local server • **Strict Reconfigure**—Number of solicit messages discarded because the client does not support reconfiguration • **Bad hardware address**—Number of packets discarded because an invalid hardware address was specified • **Bad opcode**—Number of packets discarded because an invalid operation code was specified • **Bad options**—Number of packets discarded because invalid options were specified • **Invalid server address**—Number of packets discarded because an invalid server address was specified • **No available addresses**—Number of packets discarded because there were no addresses available for assignment • **No interface match**—Number of packets discarded because they did not belong to a configured interface • **No routing instance match**—Number of packets discarded because they did not belong to a configured routing instance • **No valid local address**—Number of packets discarded because there was no valid local address • **Packet too short**—Number of packets discarded because they were too short • **Read error**—Number of packets discarded because of a system read error • **Send error**—Number of packets that the DHCPv6 local server could not send

Table 22: show dhcpv6 server statistics Output Fields *(continued)*

Field Name	Field Description
Messages received	Number of DHCPv6 messages received. • **DHCPV6_CONFIRM**—Number of DHCPv6 CONFIRM PDUs received. • **DHCPV6_DECLINE**—Number of DHCPv6 DECLINE PDUs received. • **DHCPV6_INFORMATION_REQUEST**—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • **DHCPV6_REBIND**—Number of DHCPv6 REBIND PDUs received. • **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs received. • **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs received. • **DHCPV6_RELEASE**—Number of DHCPv6 RELEASE PDUs received. • **DHCPV6_RENEW**—Number of DHCPv6 RENEW PDUs received. • **DHCPV6_REQUEST**—Number of DHCPv6 REQUEST PDUs received. • **DHCPV6_SOLICIT**—Number of DHCPv6 SOLICIT PDUs received.
Messages sent	Number of DHCPv6 messages sent. • **DHCPV6_ADVERTISE**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHCPV6_REPLY**—Number of DHCPv6 ADVERTISE PDUs transmitted. • **DHC6_RECONFIGURE**—Number of DHCPv6 RECONFIGURE PDUs transmitted.

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
    Total                0

Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
    DHCPV6_RELAY_REPL          0

Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
```


Copyright © 2011, Juniper Networks, Inc.

show esis adjacency

Syntax

show esis adjacency
<brief | detail | extensive>
<*esis-neighbor-id*>
<instance *instance-name*>
<interface *interface-name*)>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display End System-to-Intermediate System (ES-IS) adjacencies.

Options

none—(Same as **brief**) Display all ES-IS adjacencies.

brief | detail | extensive—Display the specified level of output.

esis-neighbor-id—(Optional) Display adjacencies for the specified neighbor's network service access point (NSAP) only.

instance *instance-name*—(Optional) Display adjacencies for the specified routing instance only.

interface *interface-name*—(Optional) Display adjacencies for the specified interface only.

Required Privilege Level

view

Related Documentation

- **clear esis adjacency on page 1011**

List of Sample Output

show esis adjacency on page 1178
show esis adjacency brief on page 1178
show esis adjacency detail on page 1178
show esis adjacency extensive on page 1178

Output Fields

Table 23 on page 1177 describes the output fields for the **show esis adjacency** command. Output fields are listed in the approximate order in which they appear.

Table 23: show esis adjacency Output Fields

Field Name	Field Description	Level of Output
Nbr Type	Type of network service access point (NSAP) of this neighbor.	**brief** none
NSAP/NET	NSAP of this neighbor.	All levels
Type	Type of NSAP of this neighbor.	**detail extensive**
Hold (secs)	Holdtime interval advertised by this neighbor.	**brief** none
Interface	Interface through which the neighbor is reachable.	All levels

Copyright © 2011, Juniper Networks, Inc.

Table 23: show esis adjacency Output Fields *(continued)*

Field Name	Field Description	Level of Output
Advertised holdtime	Holdtime interval advertised by this neighbor.	**detail extensive**
Expires in	How long until the adjacency expires, in seconds.	**detail extensive**
SNPA	Subnetwork point of attachment (MAC address of the neighbor).	**detail extensive**
Transition log	List of recent transitions. • **When**—Time of advertisement from this neighbor. • **State**—State of the adjacency: **Up**, **Down**, **New**, **One-way**, **Initializing**, or **Rejected**. • **Event**—Event causing the state. • **Down reason**—Reason the adjacency is down.	**extensive**

show esis adjacency

```
user@host> show esis adjacency
Nbr  NSAP/NET                                          Hold  Interface
Type                                                  (secs)
IS   47.0005.80ff.f800.0000.0108.0001.0102.5501.6008    135 fe-0/0/0.0
```

show esis adjacency brief

The output for the **show esis adjacency brief** command is identical to that for the **show esis adjacency** command. For sample output, see **show esis adjacency on page 1178**.

show esis adjacency detail

```
user@host> show esis adjacency detail
NSAP/NET: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6008, Type: IS
  Interface: fe-0/0/0.0, Advertised hold time: 180 secs, Expires in: 173 secs
  SNPA: 0:5:85:c1:73:71
```

show esis adjacency extensive

```
user@host> show esis adjacency extensive
NSAP/NET: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6008, Type: IS
  Interface: fe-0/0/0.0, Advertised hold time: 180 secs, Expires in: 167 secs
  SNPA: 0:5:85:c1:73:71
  Transition log:
  When                  State        Event           Down reason
  Sun Nov 26 22:07:35   Up           Received ISH
```


Copyright © 2011, Juniper Networks, Inc.

show esis interface

Syntax

show esis interface
<brief | detail | extensive>
<instance *instance-name*>
<interface *interface-name*)>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display End System-to-Intermediate System (ES-IS) interface information.

Options

none—(Same as **brief**) Display information for all configured ES-IS interfaces.

brief | detail | extensive—(Optional) Display the specified level of output.

instance *instance-name*—(Optional) Display configured interfaces for the specified routing instance only.

interface *interface-name*—(Optional) Display information about the specified interface only.

Required Privilege Level

view

List of Sample Output

show esis interface on page 1180
show esis interface brief on page 1180
show esis interface detail on page 1180
show esis interface extensive on page 1180

Output Fields

Table 24 on page 1179 describes the output fields for the **show esis interface** command. Output fields are listed in the approximate order in which they appear.

Table 24: show esis interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface through which the adjacency is made.	All levels
Receives	Types of hello messages that are received.	All levels
Sends	Types of hello messages that are sent.	All levels
Hello interval	Interface's hello interval, in seconds.	All levels
Adjacencies or **Num Adj**	Number of adjacencies established on this interface.	All levels
Holdtime	Interface's hold time, in seconds.	**detail extensive**
State	Internal implementation information.	**detail extensive**

Copyright © 2011, Juniper Networks, Inc.

Table 24: show esis interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
End system configuration timer	Time, in seconds, for the end system to configure itself for ES-IS.	**detail extensive**
Interface index	Index value.	**detail extensive**
NET used in hello	Network entity title used in hello messages.	**detail extensive**

show esis interface

```
user@host> show esis interface
Interface                Receives     Sends  Hello Interval  Num Adj
fe-0/0/0.0                    ISH       ISH           60.00        1
lo0.0                         ISH         -           60.00        0
```

show esis interface brief

The output for the **show esis interface brief** command is identical to that for the **show esis interface** command. For sample output, see **show esis interface on page 1180**.

show esis interface detail

```
user@host> show esis interface detail
Interface: fe-0/0/0.0
  Receives: ISH, Sends: ISH, Hello interval: 60.00
  Adjacencies: 1, Holdtime: 180, End system configuration timer: 180
  Interface index: 68, State: 0x2
  NET used in hello: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6007

Interface: lo0.0
  Receives: ISH, Sends:  - , Hello interval: 60.00
  Adjacencies: 0, Holdtime: 180, End system configuration timer: 180
  Interface index: 64, State: 0x2
  NET used in hello: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6007
```

show esis interface extensive

The output for the **show esis interface extensive** command is identical to that for the **show esis interface detail** command. For sample output, see **show esis interface detail on page 1180**.

Copyright © 2011, Juniper Networks, Inc.

show esis statistics

Syntax

show esis statistics
<instance *instance-name*>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display End System-to-Intermediate System (ES-IS) packet statistics.

Options

none—Display ES-IS packet statistics for all routing instances.

instance *instance-name*—(Optional) Display ES-IS statistics for the specified routing instance only.

Required Privilege Level

view

Related Documentation

- **clear esis statistics on page 1012**

List of Sample Output

show esis statistics on page 1181

Output Fields

Table 25 on page 1181 describes the output fields for the **show esis statistics** command. Output fields are listed in the approximate order in which they appear.

Table 25: show esis statistics Output Fields

Field Name	Field Description
PDU type	Protocol data unit type.
Received	Number of PDUs received since IS-IS started or since the statistics were set to zero.
Processed	Number of PDUs received less the number dropped.
Drops	Number of PDUs dropped.
Sent	Number of PDUs transmitted since IS-IS started or since the statistics were set to zero.
Total packets received/sent	Total number of PDUs received and transmitted since IS-IS started or since the statistics were set to zero.

show esis statistics

```
user@host> show esis statistics
PDU type  Received Processed Drops    Sent
ESH              3         3     0       8
ISH             11        10     1       4
RD               0         0     0       0
Unknown          0         0     0       0
```

```
Totals          14        13     1      12
Total packets received: 14 sent: 0
```


Copyright © 2011, Juniper Networks, Inc.

show ethernet-switching mac-learning-log

Syntax **show ethernet-switching mac-learning-log**

Release Information Command introduced in Release 9.5 of Junos OS.

Description Displays the event log of learned MAC addresses.

Required Privilege Level view

Output Fields lists the output fields for the show ethernet-switching mac-learning-log command. Output fields are listed in the approximate order in which they appear.

Table 26: show interfaces Output Fields

Field Name	Field Description
Date and Time	Timestamp when the MAC address was added or deleted from the log.
VLAN-IDX	VLAN index. An internal value assigned by Junos OS for each VLAN .
MAC	Learned MAC address.
Deleted | Added	MAC address deleted or added to the MAC learning log.
Blocking	The forwarding state of the interface: • blocked—Traffic is not being forwarded on the interface. • unblocked—Traffic is forwarded on the interface.

show ethernet-switching mac-learning-log

```
user@host> show ethernet-switching mac-learning-log
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 9 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 10 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 11 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 13 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 14 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 15 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 4 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 6 mac 00:00:00:00:00:00 was added
```

Copyright © 2011, Juniper Networks, Inc.

```
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 9 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 10 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 11 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 13 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 14 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 15 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 5 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 18 mac 00:00:05:00:00:05 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 5 mac 00:30:48:90:54:89 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 6 mac 00:00:5e:00:01:00 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:5e:00:01:08 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:5e:00:01:09 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 8 mac 00:19:e2:50:ac:00 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:5e:00:01:04 was learned
[output truncated]
```


Copyright © 2011, Juniper Networks, Inc.

show ethernet-switching table

Syntax

show ethernet-switching table
<brief | detail | extensive >
interface *interface-name* >

Release Information

Command introduced in Release 9.5 of Junos OS.

Description

Displays the Ethernet switching table.

Options

none—(Optional) Display brief information about the Ethernet-switching table.

brief | detail | extensive—(Optional) Display the specified level of output.

interface-name—(Optional) Display the Ethernet-switching table for a specific interface.

Required Privilege Level

view

Output Fields

lists the output fields for the show ethernet-switching table command. Output fields are listed in the approximate order in which they appear.

Table 27: show ethernet-switching table Output Fields

Field Name	Field Description
VLAN	The name of a VLAN.
MAC address	The MAC address associated with the VLAN.
Type	The type of MAC address. Values are: • static—The MAC address is manually created. • learn—The MAC address is learned dynamically from a packet's source MAC address. • flood—The MAC address is unknown and flooded to all members.
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).
Learned	For learned entries, the time which the entry was added to the Ethernet-switching table.

show ethernet-switching table

```
user@host> show ethernet-switching table
Ethernet-switching table: 57 entries, 17 learned
VLAN MAC address Type Age Interfaces
F2 * Flood - All-members
F2 00:00:05:00:00:03 Learn 0 ge-0/0/44.0
F2 00:19:e2:50:7d:e0 Static - Router
Linux * Flood - All-members
Linux 00:19:e2:50:7d:e0 Static - Router
Linux 00:30:48:90:54:89 Learn 0 ge-0/0/47.0
```

```
T1 * Flood - All-members
T1 00:00:05:00:00:01 Learn 0 ge-0/0/46.0
T1 00:00:5e:00:01:00 Static - Router
T1 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T1 00:19:e2:50:7d:e0 Static - Router
T10 * Flood - All-members
T10 00:00:5e:00:01:09 Static - Router
T10 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T10 00:19:e2:50:7d:e0 Static - Router
T111 * Flood - All-members
T111 00:19:e2:50:63:e0 Learn 0 ge-0/0/15.0
T111 00:19:e2:50:7d:e0 Static - Router
T111 00:19:e2:50:ac:00 Learn 0 ge-0/0/15.0
T2 * Flood - All-members
T2 00:00:5e:00:01:01 Static - Router
T2 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T2 00:19:e2:50:7d:e0 Static - Router
T3 * Flood - All-members
T3 00:00:5e:00:01:02 Static - Router
T3 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T3 00:19:e2:50:7d:e0 Static - Router
T4 * Flood - All-members
T4 00:00:5e:00:01:03 Static - Router
T4 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
[output truncated]
```

show ethernet-switching table brief

```
user@host> show ethernet-switching table brief
Ethernet-switching table: 57 entries, 17 learned
VLAN MAC address Type Age Interfaces
F2 * Flood - All-members
F2 00:00:05:00:00:03 Learn 0 ge-0/0/44.0
F2 00:19:e2:50:7d:e0 Static - Router
Linux * Flood - All-members
Linux 00:19:e2:50:7d:e0 Static - Router
Linux 00:30:48:90:54:89 Learn 0 ge-0/0/47.0
T1 * Flood - All-members
T1 00:00:05:00:00:01 Learn 0 ge-0/0/46.0
T1 00:00:5e:00:01:00 Static - Router
T1 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T1 00:19:e2:50:7d:e0 Static - Router
T10 * Flood - All-members
T10 00:00:5e:00:01:09 Static - Router
T10 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T10 00:19:e2:50:7d:e0 Static - Router
T111 * Flood - All-members
T111 00:19:e2:50:63:e0 Learn 0 ge-0/0/15.0
T111 00:19:e2:50:7d:e0 Static - Router
T111 00:19:e2:50:ac:00 Learn 0 ge-0/0/15.0
T2 * Flood - All-members
T2 00:00:5e:00:01:01 Static - Router
T2 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T2 00:19:e2:50:7d:e0 Static - Router
T3 * Flood - All-members
T3 00:00:5e:00:01:02 Static - Router
T3 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T3 00:19:e2:50:7d:e0 Static - Router
T4 * Flood - All-members
T4 00:00:5e:00:01:03 Static - Router
T4 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
[output truncated]
```


Copyright © 2011, Juniper Networks, Inc.

show ethernet-switching table detail

```
user@host> show ethernet-switching table detail
Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:05:00:00:03
Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
F2, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, 00:30:48:90:54:89
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:05:00:00:01
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
T1, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
T10, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]
```

show ethernet-switching table extensive

```
user@host> show ethernet-switching table extensive
Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:05:00:00:03
Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
```

```
F2, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, 00:30:48:90:54:89
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:05:00:00:01
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
T1, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
T10, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]
```

show ethernet-switching table interface ge-0/0/1

```
user@host> show ethernet-switching table interface ge-0/0/1
Ethernet-switching table: 1 unicast entries
VLAN     MAC address         Type     Age Interfaces
V1       *                   Flood    - All-members
V1       00:00:05:00:00:05   Learn    0 ge-0/0/1.0
```


Copyright © 2011, Juniper Networks, Inc.

show gtp tunnels

Syntax **show gtp tunnels <brief | summary>**

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display all existing GTP tunnels.

Options
- brief—Shows a short listing of all GTP tunnels
- summary—Shows a summary of all GTP tunnels

Required Privilege Level view

List of Sample Output
show gtp tunnels on page 1189
show gtp tunnels summary on page 1189

show gtp tunnels

```
user@host> show gtp tunnels

FPC 1 PIC 0:

FPC 1 PIC 1:

FPC 2 PIC 0:

FPC 2 PIC 1:

Index: 2, NSAPI: 1, Timeout: 1440m

User: 2.0.0.1/00000001 --> 3.0.0.101/00000001

Control: 2.0.0.1/00000001 --> 3.0.0.101/00000001

Index: 3, Tunnel ID: 0x0000000000000010, Timeout: 1440m

User: 2.0.0.1 --> 3.0.0.101

Control: 2.0.0.1 --> 3.0.0.101

2 tunnels active in total
```

show gtp tunnels summary

```
user@host> show gtp tunnels summary

FPC 1 PIC 0:

FPC 1 PIC 1:

FPC 2 PIC 0:

FPC 2 PIC 1:

2 tunnels active in total
```

show igmp-snooping route

Syntax

<brief | detail>
<ethernet-switching <brief | detail | vlan (*vlan-id* | *vlan-name*) >>
<inet <brief | detail |vlan (vlan-id |*vlan-name*)>>
<vlan (vlan-id | *vlan-name*)>>

Release Information

Command introduced in Release 9.5 of Junos OS.

Description

Display IGMP snooping route information.

Options

none—Display general parameters.

brief | **detail**—(Optional) Display the specified level of output.

ethernet-switching—(Optional) Display Ethernet switching information.

inet—(Optional) Display inet information.

vlan ***vlan-id*** |***vlan-name***—(Optional) Display route information for the specified VLAN.

Required Privilege Level

view

Output Fields

lists the output fields for the **show igmp-snooping route** command. Output fields are listed in the approximate order in which they appear.

Table 28: show igmp-snooping route Output Fields

Field Name	Field Description
VLAN	Name of the VLAN.
Group	Multicast group address.
Next-hop	ID associated with the next-hop device.

show igmp-snooping route

```
user@host> show igmp-snooping route
VLAN        Group           Next-hop
v11          224.1.1.1, *    533
Interfaces: ge-0/0/13.0, ge-0/0/1.0
v12          224.1.1.3, *    534
Interfaces: ge-0/0/13.0, ge-0/0/0.0
```

show igmp-snooping route vlan v1

```
user@host> show igmp-snooping route vlan v1
Table: 0
VLAN       Group               Next-hop
v1         224.1.1.1, *        1266
Interfaces: ge-0/0/0.0
v1         224.1.1.3, *        1266
Interfaces: ge-0/0/0.0
v1         224.1.1.5, *        1266
Interfaces: ge-0/0/0.0
```


Copyright © 2011, Juniper Networks, Inc.

```
v1        224.1.1.7, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.9, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.11, *      1266
Interfaces: ge-0/0/0.0
```

show igmp-snooping vlans

Syntax

show igmp-snooping vlans
<**brief** | **detail** >
<**vlan** ***vlan-id*** | ***vlan-name*** >

Release Information

Command introduced in Release 9.5 of Junos OS.

Description

Display IGMP snooping VLAN information.

Options

none—Display general parameters.

brief | **detail**—(Optional) Display the specified level of output.

vlan ***vlan-id*** | ***vlan-name*** —(Optional) Display VLAN information for the specified VLAN.

Required Privilege Level

view

Output Fields

lists the output fields for the **show igmp-snooping vlans** command. Output fields are listed in the approximate order in which they appear.

Table 29: show igmp-snooping vlans

Field Name	Field Description
VLAN	Name of the VLAN.
Interfaces	Number of interfaces in the VLAN.
Groups	Number of groups in the VLAN.
MRouters	Number of multicast routers associated with the VLAN.
Receivers	Number of host receivers in the VLAN.
Tag	Numerical identifier of the VLAN.
vlan-interface	Internal VLAN interface identifier.
Membership timeout	Membership timeout value.
Querier timeout	Timeout value for interfaces dynamically marked as router interfaces (interfaces that receive queries). When the querier timeout is reached, the switch marks the interface as a host interface.
Interface	Name of the interface.
Reporters	Number of dynamic groups on an interface.

Copyright © 2011, Juniper Networks, Inc.

show igmp-snooping vlans

```
user@host> show igmp-snooping vlans
VLAN  Interfaces  Groups  MRouters  Receivers
default  0           0       0         0
v1       11          50      0         0
v10      1           0       0         0
v11      1           0       0         0
v180     3           0       1         0
v181     3           0       0         0
v182     3           0       0         0
```

show igmp-snooping vlans vlan v10

```
user@host> show igmp-snooping vlans vlan v10
VLAN    Interfaces   Groups  MRouters   Receivers
v10     1            0       0          0
```

show igmp-snooping vlans vlan v10 detail

```
user@host> sshow igmp-snooping vlans vlan v10 detail
VLAN: v10, Tag: 10, vlan-interface: vlan.10
Membership timeout: 260, Querier timeout: 255
Interface: ge-0/0/10.0, tagged, Groups: 0, Reporters: 0
```

show interfaces

Syntax

show interfaces
< *interface-name* >
<**extensive | terse**>

Release Information

Command modified in Release 9.5 of Junos OS.

Description

Display status information and statistics about interfaces on J Series and SRX Series devices running Junos OS.

Options

interface-name —(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number. For a complete list, see the *Junos OS Interfaces Configuration Guide for Security Devices*.

- **at-*pim*/0/*port***—ATM-over-ADSL or ATM-over-SHDSL interface.
- **br-*pim*/0/*port***—Basic Rate Interface for establishing ISDN connections.
- **ce1-*pim*/0/ *port***—Channelized E1 interface.
- **cl-0/0/8**—3G wireless modem interface for SRX210 devices.
- **ct1-*pim*/0/*port***—Channelized T1 interface.
- **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
- **e1-*pim*/0/*port***—E1 interface.
- **e3-*pim*/0/*port***—E3 interface.
- **fe-*pim*/0/*port***—Fast Ethernet interface.
- **ge-*pim*/0/*port***—Gigabit Ethernet interface.
- **se-*pim*/0/*port***—Serial interface.
- **t1-*pim*/0/*port***—T1 (also called DS1) interface.
- **t3-*pim*/0/*port***—T3 (also called DS3) interface.
- **wx-*slot*/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).

extensive | terse—(Optional) Display the specified level of output.

Required Privilege Level

view

Related Documentation

- *Junos OS Interfaces Command Reference*

List of Sample Output

show interfaces Gigabit Ethernet on page 1195
show interfaces extensive (Gigabit Ethernet) on page 1195
show interfaces terse on page 1197

Copyright © 2011, Juniper Networks, Inc.

show interfaces extensive (WAN Acceleration) on page 1197
show interfaces extensive (3G Wireless Modem) on page 1198

Output Fields Table 30 on page 1195 lists the output fields for the **show interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 30: show interfaces Output Fields

Field Name	Field Description
Allowed host inbound traffic	The allowed traffic through the interface.
Traffic statistics	Number of packets and bytes transmitted and received on the physical interface.
Local statistics	Number of packets and bytes transmitted and received on the physical interface.
Transit statistics	Number of packets and bytes transiting the physical interface.
Flow input statistics	Statistics on packets received by flow module.
Flow output statistics	Statistics on packets sent by flow module.
Flow error statistics	Statistics on errors in the flow module.
Admin	The interface is enabled (up) or disabled (down).

show interfaces Gigabit Ethernet

```
user@host> show interfaces ge-0/0/1.0
Logical interface ge-0/0/1.0 (Index 67) (SNMP ifIndex 36)
      Flags: Device-Down SNMP-Traps Encapsulation: ENET2
      Protocol inet, MTU: 1500
        Flags: None
        Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
          Destination: 4.4.4/24, Local: 4.4.4.254, Broadcast: 4.4.4.255
     Security: Zone: Untrust, ident-reset: on
Allowed host-inbound traffic: bfd bgp bootp dhcp dvmrp finger ftp
                                     http https ike ident-reset igmp ldp mld
                                     msdp netconf ospf ospf3 pgm pim ping rip
                                     ripng rlogin router-discovery rpm rsh
                                     rsvp sap snmp snmp-trap ssh telnet
                                     traceroute vrrp xnm-clear xnm-sslshow
  interfaces <interface-name> extensive
```

show interfaces extensive (Gigabit Ethernet)

```
user@host> show interfaces ge-0/0/1.0 extensive
      Logical interface ge-0/0/1.0 (Index 67) (SNMP ifIndex 37) (Generation 134)

        Flags: SNMP-Traps VLAN-Tag [ 0x8100.100 ]  Encapsulation: ENET2
        Traffic statistics:
         Input  bytes  :                   0
         Output bytes  :                   0
         Input  packets:                   0
         Output packets:                   0
         Input  bytes  :              IPv6 0
         Output bytes  :              IPv6 0
         Input  packets:              IPv6 0
         Output packets:              IPv6 0
```

```
          Local statistics:
           Input  bytes  :                   0
           Output bytes  :                   0
           Input  packets:                   0
           Output packets:                   0
           Input  bytes  :              IPv6 0
           Output bytes  :              IPv6 0
           Input  packets:              IPv6 0
           Output packets:              IPv6 0
          Transit statistics:
           Input  bytes  :                   0                    0 bps
           Output bytes  :                   0                    0 bps
           Input  packets:                   0                    0 pps
           Output packets:                   0                    0 pps
           Input  bytes  :              IPv6 0
           Output bytes  :              IPv6 0
           Input  packets:              IPv6 0
           Output packets:              IPv6 0
Flow statistics:
        Flow input statistics:
         Self packets  :                   0
         ICMP packets  :                   113
         VPN packets  :                    0
         Bytes permitted by policy:        0
         Connections established:          11
        Flow output statistics:
         Multicast packets  :              0
         Bytes permitted by policy:        0
        Flow error statistics (Packets dropped due to):
         Policy denied:                    0
         No parent for a gate:             0
         Syn-attack protection:            0
         Incoming NAT errors:              0
         No session found:                 0
         No more sessions:                 0
         Invalid zone received packet:     0
         User authentication errors:       0
         Multiple user authentications:    0
         Multiple Incoming NAT:            0
         Address spoofing:                 0
         No zone or NULL zone binding      0
         No NAT gate:                      0
         No minor session:                 0
         No session for a gate:            0
         TCP sequence number out of window: 0
         No Route present:                 0
         Authentication failed:            0
         Security association not active:  0
         No SA for incoming SPI:           0
         No one interested in self packets: 0
         Protocol inet, MTU: 1500, Generation: 139, Route table: 0
           Flags: None
           Addresses, Flags: None
             Destination: Unspecified, Local: 2.2.2.2, Broadcast: Unspecified,
             Generation: 137
           Addresses, Flags: Primary Is-Primary
             Destination: Unspecified, Local: 3.3.3.3, Broadcast: Unspecified,
             Generation: 139
```


Copyright © 2011, Juniper Networks, Inc.

show interfaces terse

```
user@host> show interfaces terse
    Interface               Admin Link Proto    Local                 Remote
    ge-0/0/0                up    up
    ge-0/0/0.0              up    up   inet     10.209.4.61/18
    gr-0/0/0                up    up
    ip-0/0/0                up    up
    st0                     up    up
    st0.1                   up    ready inet
    ls-0/0/0                up    up
    lt-0/0/0                up    up
    mt-0/0/0                up    up
    pd-0/0/0                up    up
    pe-0/0/0                up    up
    e3-1/0/0                up    up
    t3-2/0/0                up    up
    e1-3/0/0                up    up
    se-4/0/0                up    down
    t1-5/0/0                up    up
    br-6/0/0                up    up
    dc-6/0/0                up    up
    dc-6/0/0.32767          up    up
    bc-6/0/0:1              down  up
    bc-6/0/0:1.0            up    down
    dl0                     up    up
    dl0.0                   up    up   inet
    dsc                     up    up
    gre                     up    up
    ipip                    up    up
    lo0                     up    up
    lo0.16385               up    up   inet     10.0.0.1            --> 0/0
                                                 10.0.0.16           --> 0/0
    lsi                     up    up
    mtun                    up    up
    pimd                    up    up
    pime                    up    up
    pp0                     up    up
```

show interfaces extensive (WAN Acceleration)

```
user@host> show interfaces wx-6/0/0 extensive
Physical interface: wx-6/0/0, Enabled, Physical link is Up
  Interface index: 142, SNMP ifIndex: 41, Generation: 143
  Type: PIC-Peer, Link-level type: PIC-Peer, MTU: 1522, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point Promiscuous SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped   : 2007-08-01 05:19:35 UTC (02:12:04 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :               58427                    0 bps
   Output bytes  :              115078                    0 bps
   Input  packets:                 847                    0 pps
   Output packets:                 972                    0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
```

```
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0
Logical interface wx-6/0/0.0 (Index 68) (SNMP ifIndex 43) (Generation 135)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PIC-Peering
    Security: Zone: wx-zone
    Allowed host-inbound traffic : any-service bootp bfd bgp  dns dvmrp
    igmp ldp msdp nhrp ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
    finger ftp tftp ident-reset http https ike netconf ping rlogin rpm rsh snmp
    snmp-trap ssh telnet traceroute xnm-clear-text xnm-ssl
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Bytes permitted by policy :       70137
      Connections established :         4
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       2866
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
      Multiple user authentications:    0
      Multiple incoming NAT:            0
      No parent for a gate:             0
      No one interested in self packets: 0
      No minor session:                 0
      No more sessions:                 0
      No NAT gate:                      0
      No route present:                 0
      No SA for incoming SPI:           0
      No tunnel found:                  0
      No session for a gate:            0
      No zone or NULL zone binding      0
      Policy denied:                    0
      Security association not active:  0
      TCP sequence number out of window: 0
      Syn-attack protection:            0
      User authentication errors:       0
    Protocol inet, MTU: 1500, Generation: 141, Route table: 0
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.87.13.2, Local: 3.3.3.3, Broadcast: Unspecified,
        Generation: 142
```

show interfaces extensive (3G Wireless Modem)

```
user@host> show interfaces cl-0/0/8 extensive
Physical interface: cl-0/0/8, Enabled, Physical link is Up
  Interface index: 67, SNMP ifIndex: 25, Generation: 4
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
  Clocking: Unspecified, Speed: MODEM
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : None
  Hold-times     : Up 0 ms, Down 0 ms
  CoS queues     : 8 supported, 8 maximum usable queues
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                    0                    0 bps
```


Copyright © 2011, Juniper Networks, Inc.

```
 Output bytes  :                  868                    0 bps
 Input  packets:                    0                    0 pps
 Output packets:                   16                    0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets

  0 best-effort               6                    6                   0
  1 expedited-fo              0                    0                   0
  2 assured-forw              0                    0                   0
  3 network-cont              10                  10                   0
MODEM status:
  Modem type                    : Sierra-USB-3G Data/Fax Modem Version 2.27m
  Initialization command string : ATS0=2
  Initialization status         : Ok
  Call status                   : Connected to 14591
  Call duration                 : 134316 seconds
  Call direction                : Dialout
  Baud rate                     : <x> bps
```

show interfaces (Aggregated Ethernet)

Syntax

show interfaces <ae*number* | reth*number* >
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index *snmp-index*>
<statistics>

Release Information

Command modified in Release 10.2 of Junos OS.

Description

Display status information about the specified aggregated Ethernet interface or redundant Ethernet interface. If you do not specify an interface name, status information for all interfaces is displayed.

Options

ae*number* | reth*number*—(Optional) Display standard information about the specified aggregated Ethernet interface or redundant Ethernet interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Aggregated Ethernet) on page 1208

Output Fields

Table 31 on page 1200 lists the output fields for the **show interfaces** (Aggregated Ethernet) command. Output fields are listed in the approximate order in which they appear.

Table 31: Aggregated Ethernet show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface and state of the interface.	All levels
Enabled	State of the physical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	All levels
Interface index	Index number of the physical interface, which reflects its initialization sequence.	All levels
SNMP ifIndex	SNMP index number for the physical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Loopback	Loopback status: **Enabled** or **Disabled**. If loopback is enabled, type of loopback: **Local** or **Remote**.	All levels
Source filtering	Source filtering status: **Enabled** or **Disabled**.	All levels
Flow control	Flow control status: **Enabled** or **Disabled**.	All levels
Minimum links needed	Number of child links that must be operational for the aggregate interface to be operational.	All levels
Device flags	Information about the physical device. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	All levels
Interface flags	Information about the interface. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	All levels
Current address	Configured MAC address.	**detail extensive**
Hardware address	Hardware MAC address.	**detail extensive**
Last flapped	Date, time, and how long ago the interface went from down to up or up to down. The format is **Last flapped:** ***year-month-day hours:minutes:seconds timezone*** **(*hours:minutes:seconds* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).**	**detail extensive**
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	**detail extensive**
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. • **Input bytes**—Number of bytes received on the interface. • **Output bytes**—Number of bytes transmitted on the interface. • **Input packets**—Number of packets received on the interface • **Output packets**—Number of packets transmitted on the interface.	**detail extensive**

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
IPv6 transit statistics	Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled. • **Input bytes**—Number of bytes received on the interface. • **Output bytes**—Number of bytes transmitted on the interface. • **Input packets**—Number of packets received on the interface. • **Output packets**—Number of packets transmitted on the interface.	**detail extensive**
Input errors	Input errors on the interface: • **Errors**—Sum of incoming frame aborts and frame check sequence (FCS) errors. • **Drops**—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • **Framing errors**—Number of packets received with an invalid FCS. • **Runts**—Number of frames received that are smaller than the runt threshold. • **Giants**—Number of frames received that are larger than the giant threshold. • **Policed discards**—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • **Resource errors**—Sum of transmit drops.	**detail extensive**
Output errors	Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious: • **Carrier transitions** —Number of times the interface has gone from **down** to **up**. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning. • **Errors**—Sum of the outgoing frame aborts and FCS errors. • **Drops**—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • **MTU errors**—Number of packets whose size exceeded the MTU of the interface. • **Resource errors**—Sum of transmit drops.	**detail extensive**
Egress queues	Total number of egress queues supported on the specified interface	**detail extensive**
Queue counters	CoS queue number and its associated user-configured forwarding class name. • **Queued packets**—Number of queued packets. • **Transmitted packets**—Number of transmitted packets. • **Dropped packets**—Number of packets dropped by the ASIC's RED mechanism.	**detail extensive**
Logical Interface		
Logical interface	Name of the logical interface.	All levels

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Index	Index number of the logical interface (which reflects its initialization sequence).	**detail extensive** none
SNMP ifIndex	SNMP interface index number of the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Flags	Information about the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	All levels
VLAN-Tag	Tag Protocol Identifier (TPID) and VLAN identifier.	All levels
Demux	IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following: • Source Family Inet • Destination Family Inet	**detail extensive** none
Encapsulation	Encapsulation on the logical interface.	All levels
Statistics	Information about the number of packets, packets per second, number of bytes, and bytes per second on this aggregate interface. • **Bundle**—Information about input and output bundle rates. • **Link**—(**detail** and **extensive** only) Information about specific links in the aggregate, including link state and input and output rates.	**detail extensive** none

LACP info	Link Aggregation Control Protocol (LACP) information for each aggregated interface.
	• **Role** can be one of the following:
	  ◦ **Actor**—Local device participating in LACP negotiation.
	  ◦ **Partner**—Remote device participating in LACP negotiation.
	• **System priority**—Priority assigned to the system (by management or administrative policy), encoded as an unsigned integer.
	• **System identifier**—Actor or partner system ID, encoded as a MAC address.
	• **Port priority**—Priority assigned to the port by the actor or partner (by management or administrative policy), encoded as an unsigned integer.
	• **Port number**—Port number assigned to the port by the actor or partner, encoded as an unsigned integer.
	• **Port key**—Operational key value assigned to the port by the actor or partner, encoded as an unsigned integer.
		detail extensive none

LACP Statistics	LACP statistics for each aggregated interface. • **LACP Rx**—LACP received counter that increments for each normal hello. • **LACP Tx**—Number of LACP transmit packet errors logged. • **Unknown Rx**—Number of unrecognized packet errors logged. • **Illegal Rx**—Number of invalid packets received.	**detail extensive** none

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Marker Statistic	(**detail** and **extensive** only) Information about 802.3ad marker protocol statistics on the specified links. • **Marker Rx**—Number of valid marker PDUs received on this aggregation port. • **Resp Tx**—Number of marker response PDUs transmitted on this aggregation port. • **Unknown Rx**—Number of frames received that either carry the slow protocols Ethernet type value (43B.4) but contain an unknown protocol data unit (PDU), or are addressed to the slow protocols group MAC address (43B.3) but do not carry the slow protocols Ethernet type. • **Illegal Rx**—Number of frames received that carry the slow protocols Ethernet type value (43B.4) but contain a badly formed PDU or an illegal value of protocol subtype (43B.4).	**detail extensive** none
Flow Statistics	Flow statistics for each aggregated interface.	**detail extensive** none
Flow Input statistics	Statistics for packets received by the flow module.	**detail extensive** none
Flow Output statistics	Statistics for packets sent by the flow module.	**detail extensive** none

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flow error statistics (Packets dropped due to)		**detail extensive** none

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output

	Packet drop statistics for the flow module.
	• **Address spoofing**—Packet dropped when the screen module detected address spoofing.
	• **Authentication failed**—Packet dropped because the IPsec Encapsulating Security Payload (ESP) or Authentication Header (AH) authentication failed.
	• **Incoming NAT errors**—Packet dropped because the source NAT rule search failed, an invalid source NAT binding was found, or the NAT allocation failed.
	• **Invalid zone received packet**—This counter is not currently in use.
	• **Multiple user authentications**—Packet dropped if it matches more than one policy that specifies user authentication. (Sometimes packets are looped through the system more than once. Each time a packet passes through the system, that packet must be permitted by a policy.)
	• **Multiple incoming NAT**—Packet dropped if source NATing is specified more than once. (Sometimes packets are looped through the system more than once.)
	• **No parent for a gate**—This counter is not currently in use.
	• **No one interested in self packets**—This counter is incremented for one of the following reasons:
	  ◦ The outbound interface is a self interface, but the packet is not marked as a to-self packet and the destination address is in a source NAT pool.
	  ◦ No service is interested in the to-self packet
	  ◦ When a zone has ident-reset service enabled, the TCP RST to IDENT request for port 113 is sent back and this counter is incremented.
	• **No minor session**—Packet dropped because no minor sessions are available and a minor session was requested. Minor sessions are allocated for storing additional TCP state information.
	• **No more sessions**—Packet dropped because there were no more free sessions available.
	• **No NAT gate**—This counter is not currently in use.
	• **No route present**—Packet dropped because a valid route was not available to forward the packet.
	• **No SA for incoming SPI**—Packet dropped because the incoming IPsec packet's security parameter index (SPI) does not match any known SPI.
	• **No tunnel found**—Packet dropped because a valid tunnel could not be found.
	• **No session for a gate**—Packet dropped by an ALG.
	• **No zone or NULL zone binding**—Packet dropped because its incoming interface was not bound to any zone.
	• **Policy denied**—The error counter is incremented for one of the following reasons:
	  ◦ Source or destination NAT (or both) has occurred and policy says to drop the packet.
	  ◦ Policy specifies user authentication, which failed.
	  ◦ Policy was configured to deny this packet.
	• **Security association not active**—Packet dropped because an IPsec packet was received for an inactive SA.
	• **TCP sequence number out of window**—TCP packet with a sequence number failed the TCP sequence number check that was received.	

Copyright © 2011, Juniper Networks, Inc.

Table 31: Aggregated Ethernet show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output

	• **Syn-attack protection**—Packet dropped because of SYN attack protection or SYN cookie protection.
	• **User authentication errors**—Packet dropped because policy requires authentication; however:
	  ◦ Only Telnet, FTP, and HTTP traffic can be authenticated.
	  ◦ The corresponding authentication entry could not be found, if web-auth is specified.
	  ◦ The maximum number of authenticated sessions per user was exceeded.	

protocol-family	Protocol family configured on the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	**brief**
Protocol	Protocol family configured on the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	**detail extensive** none
MTU	Maximum transmission unit size on the logical interface.	**detail extensive** none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Route Table	Routing table in which the logical interface address is located. For example, **0** refers to the routing table inet.0.	**detail extensive**
Flags	Information about protocol family flags. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	**detail extensive** none
Mac-Validate Failures	Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.	**detail extensive** none
Addresses, Flags	Information about address flags. For descriptions of possible values, see the "Common Output Fields" chapter in the *Junos OS Interfaces Command Reference*.	**detail extensive** none
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none
Broadcast	Broadcast address of the logical interface.	**detail extensive** none
Policer	Policer to be evaluated when packets are received or transmitted on the interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

Copyright © 2011, Juniper Networks, Inc.

show interfaces extensive (Aggregated Ethernet)

```
user@host> show interfaces ae0 extensive

Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 1973, SNMP ifIndex: 501, Generation: 2176
  Link-level type: Ethernet, MTU: 1518, Speed: 3Gbps, BPDU Error: None, MAC-REWRITE
 Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:8c:af:c0, Hardware address: 00:1f:12:8c:af:c0
  Last flapped   : 2010-04-16 14:25:36 PDT (00:02:50 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                  64                    0 bps
   Output bytes  :           9816525824            463779840 bps
   Input  packets:                   1                    0 pps
   Output packets:             38345804               226455 pps
   IPv6 transit statistics:
    Input  bytes  :                  0
    Output bytes  :                  0
    Input  packets:                  0
    Output packets:                  0
  Dropped traffic statistics due to STP State:
   Input  bytes  :                  0
   Output bytes  :                  0
   Input  packets:                  0
   Output packets:                  0
  Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
 0, Resource errors: 0
  Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets

    0 best-effort             38270790             38270790                    0

    1 expedited-fo                   0                    0                    0

    2 assured-forw                   0                    0                    0

    3 network-cont                 526                  526                    0

  Logical interface ae0.0 (Index 69) (SNMP ifIndex 502) (Generation 692)
    Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.11 ]  Encapsulation: ENET2
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :             1          0            64            0
        Output:      38572259     226453    9874497884    463775744
    Link:
      ge-5/0/1.0
        Input :             0          0             0            0
        Output:      12743866      75484    3262429696    154591232
      ge-5/2/0.0
        Input :             1          0            64            0
        Output:      13043256      75484    3339073116    154591232
      ge-5/2/1.0
        Input :             0          0             0            0
        Output:      12785137      75485    3272995072    154593280
```


Copyright © 2011, Juniper Networks, Inc.

```
    Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
      ge-5/0/1.0                0           0            0            0
      ge-5/2/0.0                0           0            0            0
      ge-5/2/1.0                0           0            0            0
    Security: Zone: HOST
    Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
    finger ftp tftp ident-reset http https ike netconf ping reverse-telnet
reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet
    traceroute xnm-clear-text xnm-ssl lsping ntp sip
    Flow Statistics :
    Flow Input statistics :
      Self packets :                     0
      ICMP packets :                     0
      VPN packets :                      0
      Multicast packets :                0
      Bytes permitted by policy :        0
      Connections established :          0
    Flow Output statistics:
      Multicast packets :                0
      Bytes permitted by policy :        8976842784
    Flow error statistics (Packets dropped due to):
      Address spoofing:                  0
      Authentication failed:             0
      Incoming NAT errors:               0
      Invalid zone received packet:      0
      Multiple user authentications:     0
      Multiple incoming NAT:             0
      No parent for a gate:              0
      No one interested in self packets: 0
      No minor session:                  0
      No more sessions:                  0
      No NAT gate:                       0
      No route present:                  0
      No SA for incoming SPI:            0
      No tunnel found:                   0
      No session for a gate:             0
      No zone or NULL zone binding       0
      Policy denied:                     0
      Security association not active:   0
      TCP sequence number out of window: 0
      Syn-attack protection:             0
      User authentication errors:        0
    Protocol inet, MTU: 1500, Generation: 841, Route table: 0
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 100.1.1/24, Local: 100.1.1.2, Broadcast: 100.1.1.255,
Generation: 422
    Protocol multiservice, MTU: Unlimited, Generation: 842, Route table: 0
      Flags: Is-Primary
      Policer: Input: __default_arp_policer__
   Logical interface ae0.32767 (Index 83) (SNMP ifIndex 503) (Generation 693)
    Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ]  Encapsulation: ENET2
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :             0          0             0            0
        Output:             0          0             0            0
    Link:
      ge-5/0/1.32767
        Input :             0          0             0            0
        Output:             0          0             0            0
```

```
    ge-5/2/0.32767
      Input :             0          0             0            0
      Output:             0          0             0            0
    ge-5/2/1.32767
      Input :             0          0             0            0
      Output:             0          0             0            0
  LACP info:        Role     System             System      Port    Port  Port

                           priority         identifier  priority  number   key

    ge-5/0/1.32767    Actor      127 00:1f:12:8c:af:c0       127     833     1

    ge-5/0/1.32767  Partner      127 00:1f:12:8f:d7:c0       127     641     1

    ge-5/2/0.32767    Actor      127 00:1f:12:8c:af:c0       127     848     1

    ge-5/2/0.32767  Partner      127 00:1f:12:8f:d7:c0       127     656     1

    ge-5/2/1.32767    Actor      127 00:1f:12:8c:af:c0       127     849     1

    ge-5/2/1.32767  Partner      127 00:1f:12:8f:d7:c0       127     657     1

  LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
    ge-5/0/1.32767           342         511            0            0
    ge-5/2/0.32767           344         498            0            0
    ge-5/2/1.32767           344         500            0            0
  Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
    ge-5/0/1.32767             0           0            0            0
    ge-5/2/0.32767             0           0            0            0
    ge-5/2/1.32767             0           0            0            0
  Security: Zone: HOST
  Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
  finger ftp tftp ident-reset http https ike netconf ping reverse-telnet
reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet
  traceroute xnm-clear-text xnm-ssl lsping ntp sip
  Flow Statistics :
  Flow Input statistics :
    Self packets :                     0
    ICMP packets :                     0
    VPN packets :                      0
    Multicast packets :                0
    Bytes permitted by policy :        0
    Connections established :          0
  Flow Output statistics:
    Multicast packets :                0
    Bytes permitted by policy :        0
  Flow error statistics (Packets dropped due to):
    Address spoofing:                  0
    Authentication failed:             0
    Incoming NAT errors:               0
    Invalid zone received packet:      0
    Multiple user authentications:     0
    Multiple incoming NAT:             0
    No parent for a gate:              0
    No one interested in self packets: 0
    No minor session:                  0
    No more sessions:                  0
    No NAT gate:                       0
    No route present:                  0
    No SA for incoming SPI:            0
```


Copyright © 2011, Juniper Networks, Inc.

```
  No tunnel found:                  0
  No session for a gate:            0
  No zone or NULL zone binding      0
  Policy denied:                    0
  Security association not active:  0
  TCP sequence number out of window: 0
  Syn-attack protection:            0
  User authentication errors:       0
Protocol multiservice, MTU: Unlimited, Generation: 843, Route table: 0
  Flags: None
  Policer: Input: __default_arp_policer__
```

show interfaces flow-statistics

Syntax **show interfaces flow-statistics** *<interface-name>*

Release Information Command introduced in Release 8.5 of Junos OS.

Description Display interfaces flow statistics.

Options *Interface-name*—(Optional) Display flow statistics about the specified interface. Following is a list of typical interface names. Replace *pim* with the PIM slot and *port* with the port number. For a complete list, see the *Junos OS Interfaces Configuration Guide for Security Devices*.

- **at-*pim*/0/*port***—ATM-over-ADSL or ATM-over-SHDSL interface.
- **br-*pim*/0/*port***—Basic Rate Interface for establishing ISDN connections.
- **ce1-*pim*/0/*port***—Channelized E1 interface.
- **ct1-*pim*/0/*port***—Channelized T1 interface.
- **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
- **e1-*pim*/0/*port***—E1 interface.
- **e3-*pim*/0/*port***—E3 interface.
- **fe-*pim*/0/ *port***—Fast Ethernet interface.
- **ge-*pim*/0/*port***—Gigabit Ethernet interface.
- **se-*pim*/0/*port***—Serial interface.
- **t1-*pim*/0/*port***—T1 (also called DS1) interface.
- **t3-*pim*/0/ *port***—T3 (also called DS3) interface.
- **wx-*slot*/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).

Required Privilege Level view

List of Sample Output **show interfaces flow-statistics (Gigabit Ethernet) on page 1215**

Output Fields Table 32 on page 1212 lists the output fields for the **show interfaces flow-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 32: show interfaces flow-statistics Output Fields

Field Name	Field Description
Traffic statistics	Number of packets and bytes transmitted and received on the physical interface.
Local statistics	Number of packets and bytes transmitted and received on the physical interface.

 Copyright © 2011, Juniper Networks, Inc.

Table 32: show interfaces flow-statistics Output Fields *(continued)*

Field Name	Field Description
Transit statistics	Number of packets and bytes transiting the physical interface.
Flow input statistics	Statistics on packets received by flow module.
Flow output statistics	Statistics on packets sent by flow module.
Flow error statistics	Packet drop statistics for the flow module. For further detail, see Table 33 on page 1213

Table 33: Flow Error Statistics (packet drop statistics for the flow module)

Error	Error Description
Screen:	
Address spoofing	The packet was dropped when the screen module detected address spoofing.
Syn-attack protection	The packet was dropped because of SYN attack protection or SYN cookie protection.
VPN:	
Authentication failed	The packet was dropped because the IPsec Encapsulating Security Payload (ESP) or Authentication Header (AH) authentication failed.
No SA for incoming SPI	The packet was dropped because the incoming IPsec packet's security parameter index (SPI) does not match any known SPI.
Security association not active	The packet was dropped because an IPsec packet was received for an inactive SA.
NAT:	
Incoming NAT errors	The source NAT rule search failed, an invalid source NAT binding was found, or the NAT allocation failed.
Multiple incoming NAT	Sometimes packets are looped through the system more than once; if source NATing is specified more than once, the packet will be dropped.
Auth:	
Multiple user authentications	Sometimes packets are looped through the system more than once. Each time a packet passes through the system, that packet must be permitted by a policy. If the packet matches more than one policy that specifies user authentication, then it will be dropped.
User authentication errors	Packet was dropped because policy requires authentication; however: • Only Telnet, FTP, and HTTP traffic can be authenticated. • The corresponding authentication entry could not be found, if web-auth is specified. • The maximum number of authenticated sessions per user was exceeded.
Flow:	

Table 33: Flow Error Statistics (packet drop statistics for the flow module) *(continued)*

No one interested in self packets	This counter is incremented for one of the following reasons: • The outbound interface is a self interface, but the packet is not marked as a to-self packet and the destination address is in a source NAT pool. • No service is interested in the to-self packet • When a zone has ident-reset service enabled, the TCP RST to IDENT request for port 113 is sent back and this counter is incremented.
No minor session	The packet was dropped because no minor sessions are available and a minor session was requested. Minor sessions are allocated for storing additional TCP state information.
No more sessions	The packet was dropped because there were no more free sessions available.
No route present	The packet was dropped because a valid route was not available to forward the packet. For new sessions, the counter is incremented for one of the following reasons: • No valid route was found to forward the packet. • A discard or reject route was found. • The route could not be added due to lack of memory. • The reverse path forwarding check failed for an incoming multicast packet. For existing sessions, the prior route was changed or deleted, or a more specific route was added. The session is rerouted, and this reroute could fail because: • A new route could not be found; either the previous route was removed, or the route was changed to discard or reject. • Multiple packets may concurrently force rerouting to occur, and only one packet can successfully complete the rerouting process. Other packets will be dropped. • The route table was locked for updates by the routing engine. Packets that match a new session are retried, whereas packets that match an existing session are not.
No tunnel found	The packet was dropped because a valid tunnel could not be found
No session for a gate	This counter is incremented when a packet is destined for an ALG, and the ALG decides to drop this packet.
No zone or NULL zone binding	The packet was dropped because its incoming interface was not bound to any zone.
Policy denied	The error counter is incremented for one of the following reasons: • Source and/or destination NAT has occurred and policy says to drop the packet. • Policy specifies user authentication, which failed. • Policy was configured to deny this packet.
TCP sequence number out of window	A TCP packet with a sequence number failed the TCP sequence number check that was received.
Counters Not Currently in Use	
No parent for a gate	-
Invalid zone received packet	-

Copyright © 2011, Juniper Networks, Inc.

Table 33: Flow Error Statistics (packet drop statistics for the flow module) *(continued)*

No NAT gate	-

show interfaces flow-statistics (Gigabit Ethernet)

```
user@host> show interfaces flow-statistics ge-0/0/1.0
  Logical interface ge-0/0/1.0 (Index 70) (SNMP ifIndex 49)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 5161
    Output packets: 83
    Security: Zone: zone2
    Allowed host-inbound traffic : bootp bfd bgp  dns dvmrp igmp ldp msdp nhrp
ospf pgm
    pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset http
 https ike
   netconf ping rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
 xnm-ssl
    lsping
    Flow Statistics :
    Flow Input statistics :
      Self packets :                     0
      ICMP packets :                     0
      VPN packets :                      2564
      Bytes permitted by policy :        3478
      Connections established :          1
    Flow Output statistics:
      Multicast packets :                0
      Bytes permitted by policy :        16994
    Flow error statistics (Packets dropped due to):
      Address spoofing:                  0
      Authentication failed:             0
      Incoming NAT errors:               0
      Invalid zone received packet:      0
      Multiple user authentications:     0
      Multiple incoming NAT:             0
      No parent for a gate:              0
      No one interested in self packets: 0
      No minor session:                  0
      No more sessions:                  0
      No NAT gate:                       0
      No route present:                  0
      No SA for incoming SPI:            0
      No tunnel found:                   0
      No session for a gate:             0
      No zone or NULL zone binding       0
      Policy denied:                     0
      Security association not active:   0
      TCP sequence number out of window: 0
      Syn-attack protection:             0
      User authentication errors:        0
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 2.2.2/24, Local: 2.2.2.2, Broadcast: 2.2.2.255
```

show interfaces swfabx

Syntax show interfaces <swfab0 | swfab1>

Release Information Command introduced in Release 11.1 of Junos OS.

Description List the configured interfaces for each swfab interface. The swfab interface can contain one or more members because it is an aggregated interface.

Required Privilege Level view

Related Documentation

- **clear interfaces statistics swfabx on page 1014**

List of Sample Output **show interfaces <swfab0 | swfab1> on page 1216**

Output Fields Table 34 on page 1216 lists the output fields for the **show interfaces <swfab0 | swfab1>** command. Output fields are listed in the approximate order in which they appear.

Table 34: show interfaces <swfab0 | swfab1> Output Fields

Field Name	Field Description
fabric-options	The fabric-options hierarchy is made to be in sync with the fab interfaces.
member-interfaces	Interfaces specified under member-interfaces are single logical aggregate-Ethernet interfaces. This interface carries internode switching traffic.

show interfaces <swfab0 | swfab1>

```
user@host> show interfaces <swfab0 | swfab1>
fabric-options {
       member-interfaces {
           ge-0/0/6;
           ge-0/0/7;
       }
  }
```


Copyright © 2011, Juniper Networks, Inc.

show lacp interfaces

Syntax **show lacp interfaces** <*interface-name*>

Release Information Command modified in Release 10.2 of Junos OS.

Description Display Link Aggregation Control Protocol (LACP) information about the specified aggregated Ethernet interface, redundant Ethernet interface, Gigabit Ethernet interface, or 10-Gigabit Ethernet interface. If you do not specify an interface name, LACP information for all interfaces is displayed.

Options *interface-name*—(Optional) Display LACP information for the specified interface:

- Aggregated Ethernet—**ae*number***
- Redundant Ethernet—**reth*number***
- Gigabit Ethernet—**ge-*fpc/pic/port***
- 10-Gigabit Ethernet—**xe*number***

Required Privilege Level view

List of Sample Output **show lacp interfaces (Aggregated Ethernet) on page 1219**
show lacp interfaces (Redundant Ethernet) on page 1220
show lacp interfaces (Gigabit Ethernet) on page 1220

Output Fields Table 35 on page 1217 lists the output fields for the **show lacp interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 35: show lacp interfaces Output Fields

Field Name	Field Description
Aggregated interface	Aggregated interface value.

Table 35: show lacp interfaces Output Fields *(continued)*

Field Name	Field Description

LACP State	LACP state information for each aggregated interface:
	• **Role**—Role played by the interface. It can be one of the following:
	  ◦ **Actor**—Local device participating in LACP negotiation.
	  ◦ **Partner**—Remote device participating in LACP negotiation.
	• **Exp**—Expired state. **Yes** indicates the actor or partner is in an expired state. **No** indicates the actor or partner is not in an expired state.
	• **Def**—Default. **Yes** indicates that the actor's receive machine is using the default operational partner information, administratively configured for the partner. **No** indicates the operational partner information in use has been received in a link aggregation control protocol data unit (PDU).
	• **Dist**—Distribution of outgoing frames. **No** indicates distribution of outgoing frames on the link is currently disabled and is not expected to be enabled. Otherwise, the value is **Yes**.
	• **Col**—Collection of incoming frames. **Yes** indicates collection of incoming frames on the link is currently enabled and is not expected to be disabled. Otherwise, the value is **No**.
	• **Syn**—Synchronization. If the value is **Yes**, the link is considered synchronized. It has been allocated to the correct link aggregation group, the group has been associated with a compatible aggregator, and the identity of the link aggregation group is consistent with the system ID and operational key information transmitted. If the value is **No**, the link is not synchronized. It is currently not in the right aggregation.
	• **Aggr**—Ability of aggregation port to aggregate (**Yes**) or to operate only as an individual link (**No**).
	• **Timeout**—LACP timeout preference. Periodic transmissions of link aggregation control PDUs occur at either a slow or fast transmission rate, depending upon the expressed LACP timeout preference (**Long Timeout** or **Short Timeout**).
	• **Activity**—Actor or partner's port activity. **Passive** indicates the port's preference for not transmitting link aggregation control PDUs unless its partner's control value is **Active**. **Active** indicates the port's preference to participate in the protocol regardless of the partner's control value.

Copyright © 2011, Juniper Networks, Inc.

Table 35: show lacp interfaces Output Fields *(continued)*

Field Name	Field Description

LACP Protocol	LACP protocol information for each aggregated interface:
	• Link state (active or standby) indicated in parentheses next to the interface when link protection is configured.
	• **Receive State**—One of the following values:
	  • **Current**—The state machine receives a link aggregation control PDU and enters the **Current** state.
	  • **Defaulted**—If no link aggregation control PDU is received before the timer for the **Current** state expires a second time, the state machine enters the **Defaulted** state.
	  • **Expired**—If no link aggregation control PDU is received before the timer for the **Current** state expires once, the state machine enters the **Expired** state.
	  • **Initialize**—When the physical connectivity of a link changes or a Begin event occurs, the state machine enters the **Initialize** state.
	  • **LACP Disabled**—If the port is operating in half duplex, the operation of LACP is disabled on the port, forcing the state to **LACP Disabled**. This state is similar to the **Defaulted** state, except that the port is forced to operate as an individual port.
	  • **Port Disabled**—If the port becomes inoperable and a Begin event has not occurred, the state machine enters the **Port Disabled** state.
	• **Transmit State**—Transmit state of state machine. One of the following values:
	  • **Fast Periodic**—Periodic transmissions are enabled at a fast transmission rate.
	  • **No Periodic**—Periodic transmissions are disabled.
	  • **Periodic Timer**—Transitory state entered when the periodic timer expires.
	  • **Slow Periodic**—Periodic transmissions are enabled at a slow transmission rate.
	• **Mux State**—State of the multiplexer state machine for the aggregation port. The state is one of the following values:
	  • **Attached**—Multiplexer state machine initiates the process of attaching the port to the selected aggregator.
	  • **Collecting Distributing**—Collecting and distributing states are merged together to form a combined state (coupled control). Because independent control is not possible, the coupled control state machine does not wait for the partner to signal that collection has started before enabling both collection and distribution.
	  • **Detached**—Process of detaching the port from the aggregator is in progress.
	  • **Waiting**—Multiplexer state machine is in a holding process, awaiting an outcome.

show lacp interfaces (Aggregated Ethernet)

```
user@host> show lacp interfaces ae0
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-2/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-2/0/0                  Current   Fast periodic Collecting distributing
      ge-2/0/1                  Current   Fast periodic Collecting distributing
      ge-2/2/0                  Current   Fast periodic Collecting distributing
      ge-2/2/1                  Current   Fast periodic Collecting distributing
```

show lacp interfaces (Redundant Ethernet)

```
user@host> show lacp interfaces reth0
Aggregated interface: reth0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-11/0/0      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/0    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/1      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/1    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/2      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/2    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/3      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/3    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/2       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/2     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/3       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/3     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-11/0/0                Current   Fast periodic Collecting distributing
      ge-11/0/1                Current   Fast periodic Collecting distributing
      ge-11/0/2                Current   Fast periodic Collecting distributing
      ge-11/0/3                Current   Fast periodic Collecting distributing
      ge-3/0/0                 Current   Fast periodic Collecting distributing
      ge-3/0/1                 Current   Fast periodic Collecting distributing
      ge-3/0/2                 Current   Fast periodic Collecting distributing
      ge-3/0/3                 Current   Fast periodic Collecting distributing
{primary:node1}
```

show lacp interfaces (Gigabit Ethernet)

```
user@host> show lacp interfaces ge-0/3/0
Aggregated interface: ae0
    LACP State:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/3/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/3/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP Protocol:   Receive State    Transmit State          Mux State
      ge-0/3/0             Current     Fast periodic  Collecting distributing
```


Copyright © 2011, Juniper Networks, Inc.

show lacp statistics interfaces

Syntax **show lacp statistics interfaces** <*interface-name*>

Release Information Command modified in Release 10.2 of Junos OS.

Description Display Link Aggregation Control Protocol (LACP) statistics about the specified aggregated Ethernet interface or redundant Ethernet interface. If you do not specify an interface name, LACP statistics for all interfaces are displayed.

Options *interface-name*—(Optional) Name of an interface.

Required Privilege Level view

List of Sample Output **show lacp statistics interfaces on page 1221**

Output Fields Table 36 on page 1221 lists the output fields for the **show lacp statistics interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 36: show lacp statistics interfaces Output Fields

Field Name	Field Description
Aggregated interface	Aggregated interface value.
LACP Statistics	LACP statistics provide the following information: • **LACP Rx**—LACP received counter that increments for each normal hello. • **LACP Tx**—Number of LACP transmit packet errors logged. • **Unknown Rx**—Number of unrecognized packet errors logged. • **Illegal Rx**—Number of invalid packets received.

show lacp statistics interfaces

```
user@host> show lacp statistics interfaces ae0
Aggregated interface: ae0
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-2/0/0                1352        2035            0            0
      ge-2/0/1                1352        2056            0            0
      ge-2/2/0                1352        2045            0            0
      ge-2/2/1                1352        2043            0            0
```

show modem wireless interface

Syntax **show modem wireless interface *interface-name***

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display information about 3G wireless modem interface.

Options **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

Required Privilege Level view

List of Sample Output **show modem wireless interface cl-0/0/8 on page 1222**

Output Fields Table 37 on page 1222 lists the output fields for the **show modem wireless interface** command.

Table 37: show modem wireless interface Output Fields

Field Name	Field Description
Wireless modem firmware details	Display firmware information about the 3G wireless modem. See **show modem wireless interface firmware**.
Wireless Modem Network Info	Display network statistics for the 3G wireless modem interface. See **show modem wireless interface network**.
Radio statistics	Display received signal strength indication (RSSI) for the 3G wireless modem. See **show modem wireless interface rssi**.

show modem wireless interface cl-0/0/8

```
user@host> show modem wireless interface cl-0/0/8
Wireless modem firmware details
  Modem firmware version: F1_2_3_15AP C:/WS/FW/F1_2_3_15AP/MSM7200R3/SRC/AMSS
2008/07/09 12:22:16
  Modem Firmware build date: 07/09/08
  Card type: Aircard 880E
  Modem manufacturer: Sierra Wireless, Inc
  Hardware version: 1.0
  Factory serial number (FSN): D46031822831022W
  Modem PIN security status: Disabled.
  SIM Status: SIM Okay
  SIM lock: Unlocked
  SIM user operation needed: No Op
  Retries remaining: 3
  Current modem temperature: 25 deg C
Wireless Modem Network Info
  Current Modem Status: Online
  Current Service Status: Offline
  Current Service Type: Combo(CS,PS)
  Current Service Mode: HSPA
  Current Band: 257.
  Roaming Status: No
```

 Copyright © 2011, Juniper Networks, Inc.

```
  Network Selection Mode: Automatic
  Network:
  Mobile Country Code (MCC): 1
  Mobile Network Code (MNC): 1
  Location Area Code (LAC): 128
  Routing Area Code (RAC): 0
  Cell Identification: 0
  Scrambling Code: 9
Radio statistics
  Current radio signal strength: -95 dB
```

show modem wireless interface firmware

Syntax **show modem wireless interface *interface-name* firmware**

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display firmware details for 3G wireless modem interface.

Options **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

Required Privilege Level view

List of Sample Output **show modem wireless interface firmware (CDMA EV-DO modem) on page 1225**
show modem wireless interface firmware (GSM modem) on page 1225

Output Fields Table 38 on page 1224 lists some of the output fields for the **show modem wireless interface firmware** command. Output fields are listed in the approximate order in which they appear.

Table 38: show modem wireless interface firmware Output Fields

Field Name	Field Description
SIM Status	Status of the subscriber identity module (SIM) in the GSM 3G wireless modem card. The status can be one of the following states: • **SIM Okay** • **SIM not inserted** • **SIM removed** • **SIM init failure**—There is a problem with the SIM; the SIM may need to be replaced. • **SIM locked** • **PIN1 blocked**—Obtain a PIN unblocking key (PUK) to unblock the SIM. • **PIN1 rejected**—The wrong PIN was entered. • **PIN2 rejected**—The wrong PIN was entered. • **Network rejected**
SIM lock	Whether the SIM is locked or unlocked. See **SIM user operation needed** to determine if any action is required.
SIM user operation needed	Action required by the user. This can be one of the following: • **No op**—No user operation required. • **Enter PIN**—Enter the personal identification number (PIN) to unlock the SIM. See **request modem wireless gsm sim-unlock**. • **Enter PUK**—Enter the PIN unblocking key (PUK) to unblock the SIM. See **request modem wireless gsm sim-unblock**.

 Copyright © 2011, Juniper Networks, Inc.

Table 38: show modem wireless interface firmware Output Fields *(continued)*

Field Name	Field Description
Retries remaining	If the value of **SIM user operation needed** is **Enter PIN**, the number of PIN unlock attempts remaining before the modem is blocked. If the PIN is entered incorrectly three consecutive times, the SIM is blocked. If the value of **SIM user operation needed** is **Enter PUK**, the number of unblock attempts remaining before the modem is unusable. If the PUK is entered incorrectly ten times, the SIM must be returned to the service provider for reactivation.

show modem wireless interface firmware (CDMA EV-DO modem)

```
user@host> show modem wireless interface cl-0/0/8 firmware
Modem Firmware Version : p2005600
    Modem Firmware built date : 12-09-07
    Card type : Aircard 597E - CDMA EV-DO revA
    Manufacturer : Sierra Wireless, Inc.
    Hardware Version : 1.0
    Electronic Serial Number (ESN) : 0x6032688F
    Preferred Roaming List (PRL) Version : 20224
    Supported Mode : 1xev-do rev-a, 1x
    Current Modem Temperature : 32 C
    Modem Activated : YES
    Activation Date: 2-06-08
    Modem PIN Security : Unlocked
    Power-up lock : Disabled
```

show modem wireless interface firmware (GSM modem)

```
user@host> show modem wireless interface cl-0/0/8 firmware
  Wireless modem firmware details
   Modem firmware version: F1_2_3_15AP C:/WS/FW/F1_2_3_15AP/MSM7200R3/SRC/AMSS
2008/07/09 12:22:16
   Modem Firmware build date: 07/09/08
   Card type: Aircard 881E
   Modem manufacturer: Sierra Wireless, Inc
   Hardware version: 1.0
   Factory serial number (FSN): D46031813941022W
   Modem PIN security status: Disabled
   SIM status: Low Power
   SIM lock: Unlocked
   SIM user operation needed: No Op
   Retries remaining: 3
   Current modem temperature: 25 degrees Celsius
```

Copyright © 2011, Juniper Networks, Inc.

show modem wireless interface network

Syntax **show modem wireless interface *interface-name* network**

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display wireless network statistics for 3G wireless modem interface.

Options **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

Required Privilege Level view

List of Sample Output **show modem wireless interface network (CDMA EV-DO modem) on page 1227**
show modem wireless interface network (GSM modem) on page 1227

Output Fields Table 39 on page 1226 lists some of the output fields for the **show modem wireless interface network** command.

Table 39: show modem wireless interface network Output Fields

Field Name	Field Description
System Identifier (SID)	Current SID of the network providing service.
Network Identifier (SID)	Current NID of the station providing service.
Roaming Status	Roaming state.
Current Modem Status	Status of the 3G wireless modem card. The status can be one of the following states: • **Offline**—Modem is not usable • **Online**—Modem booted properly • **Low Power**—Modem booted and in low power mode
Current Service Status	Status of the 3G wireless modem connection. The status can be one of the following states: • **Offline**—Modem is not connected • **Online**—Modem is connected
Current Service Type	One of the following: • Circuit switched (CS) • Packet switched (PS • Combo (CS,PS)

 Copyright © 2011, Juniper Networks, Inc.

Table 39: show modem wireless interface network Output Fields *(continued)*

Field Name	Field Description
Current Service Mode	One of the following: • High-Speed Packet Access (HSPA) • High-Speed Downlink Packet Access (HSDPA) • High-Speed Uplink Packet Access (HSUPA)
Current Band	Current radio band in use.
Mobile country Code (MCC)	Number that uniquely identifies the country.
Mobile Network Code	Number that uniquely identifies a network within a country.
System Identifier (SID)	Current SID of the network providing service.

show modem wireless interface network (CDMA EV-DO modem)

```
user@host> show modem wireless interface cl-0/0/8 network
Running Operating mode : 1xEV-DO (Rev A) and 1xRTT
 Call Setup Mode : Mobile IP only
 System Identifier (SID) : 3421
 Network Identifier (NID) : 91
 Roaming Status(1xRTT) : Home
 Idle Digital Mode : HDR
 System Time : Wed Jun6 15:16:9 2008
```

show modem wireless interface network (GSM modem)

```
user@host> show modem wireless interface cl-0/0/8 network
Wireless Modem Network Info
   Current Modem Status: Online
   Current Service Status: Offline
   Current Service Type: Combo(CS,PS)
   Current Service Mode: HSPA
   Current Band: 257
   Roaming Status: No
   Network Selection Mode: Automatic
   Network:
   Mobile Country Code (MCC): 1
   Mobile Network Code (MNC): 1
   Location Area Code (LAC): 128
   Routing Area Code (RAC): 0
   Cell Identification: 0
   Scrambling Code: 9
```

Copyright © 2011, Juniper Networks, Inc.

show modem wireless interface rssi

Syntax **show modem wireless interface *interface-name* rssi**

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display received signal strength indication (RSSI) for 3G wireless modem interface.

Options **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

Required Privilege Level view

List of Sample Output **show modem wireless interface cl-0/0/8 rssi on page 1228**

Output Fields Table 40 on page 1228 lists the output fields for the **show modem wireless interface rssi** command.

Table 40: show modem wireless interface rssi Output Fields

Field Name	Field Description
rssi	Current RSSI, in decibels (dB).

show modem wireless interface cl-0/0/8 rssi

```
user@host> show modem wireless interface cl-0/0/8 rssi
Radio statistics
  Current radio signal strength: -95 dB
```


Copyright © 2011, Juniper Networks, Inc.

show network-access address-assignment pool

Syntax show network-access address-assignment pool *name*

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display information summary about a specific pool.

Required Privilege Level view

Output Fields Table 41 on page 1229 lists the output fields for the **show network-access address-assignment pool** command. Output fields are listed in the approximate order in which they appear.

Table 41: show network-access address-assignment pool Output Fields

Field Name	Field Description
IP address	IP address assigned to a client.
Hardware address	MAC address of the client. For XAuth clients, the value is NA.
Host/User	For static IP address assignment, the user name and profile are displayed in the format *username@profile*. If the client is assigned an IP address from an address pool and a user name exists, the user name is displayed. For DHCP applications, if the host name is configured the host name is displayed; otherwise NA is displayed.
Type	Either XAuth or DHCP attributes are configured.

Sample Output

```
user@host> show network-access address-assignment pool xauth1
IP address       Hardware address       Host/User                Type
40.0.0.1         NA                     jason@dvpn-auth          XAUTH
40.0.0.2         NA                     jacky                    XAUTH
40.0.0.3         00:05:1b:00:b9:01      host1                    DHCP
40.0.0.4         00:05:1b:00:b9:02      NA                       DHCP
```

Copyright © 2011, Juniper Networks, Inc.

show network-access requests pending

Syntax

show network-access requests pending
<**detail**>
<**index** *number* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display the status of pending authentication requests.

Options

none—Show pending authentication requests.

detail—Display detailed information about all pending requests.

index *number* —(Optional) Display detailed information about the request specified by this index number. Use the command without options to obtain a list of requests and index numbers.

Required Privilege Level

view

Related Documentation

- **clear network-access requests pending on page 1016**

List of Sample Output

show network-access requests pending on page 1231
show network-access requests pending detail on page 1231
show network-access requests pending index 1 on page 1231

Output Fields

Table 42 on page 1230 lists the output fields for the show network-access requests pending command. Output fields are listed in the approximate order in which they appear.

Table 42: show network-access requests pending Output Fields

Field Name	Field Description
Index	Internal number identifying the pending request. Use this number to obtain more information on the record.
User	Originator of authentication request.
Status	The pending requests are requests and responses that are not yet sent back to the respective clients. The pending requests can be in one of the following states: • **Processing**: This request is being processed by the device. The authentication process has started but is not complete. • **Waiting on Auth Server**: The request is sent to an external authentication server, and the device is waiting for the response. • **Processed:** This request has completed authentication (success or failure). The results are not yet forwarded back to the client. • **Request cancelled by Admin**: This request was cancelled by the Admin. The reply with cancel code is not yet sent back to the client.

Copyright © 2011, Juniper Networks, Inc.

Table 42: show network-access requests pending Output Fields *(continued)*

Field Name	Field Description
Profile	The profile determines how the user is authenticated. Local clients defined with the statement **access profile client** are authenticated with the password authentication. Clients configured external to the device, on a RADIUS or LDAP server are authenticated with RADIUS or LDAP authentication.

show network-access requests pending

```
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                  Status
1     Sun                   Processing
2     Sam                   Processed
```

show network-access requests pending detail

```
user@host> show network-access requests pending detail
Information about pending authentication entries
  Total pending authentication requests: 2
Index: 1  User: Sun
  Status: Processing
  Profile: Sunnyvale-firewall-users
Index: 2  User: Sam
  Status: Processed
  Profile: Westford-profile
```

show network-access requests pending index 1

```
user@host> show network-access requests pending index 1
Index: 1  User: Sun
  Status: Processing
  Profile: Sunnyvale-firewall-users
```

Copyright © 2011, Juniper Networks, Inc.

show network-access requests statistics

Syntax **show network-access requests statistics**

Release Information Command modified in Release 9.1 of Junos OS.

Description Display authentication statistics for the configured authentication type.

Required Privilege Level view

Related Documentation

- **authentication-order on page 12**
- **clear network-access requests statistics on page 1017**

Output Fields Table 43 on page 1232 lists the output fields for the network-access requests statisticscommand. Output fields are listed in the approximate order in which they appear.

Table 43: show network-access requests statistics Output Fields

Field Name	Field Description
Total requests received	Total number of authentication requests that the device received from clients.
Total responses sent	Total number of authentication responses that the device sent to the clients.
Success responses	Total number of clients that authenticated successfully.
Failure responses	Total number of clients that failed to authenticate.

show network-access requests statistics

```
user@host> show network-access requests statistics
General authentication statistics
  Total requests received: 100
  Total responses sent: 70
Radius authentication statistics
  Total requests received: 40
  Success responses: 20
  Failure responses: 20
LDAP authentication statistics
  Total requests received: 30
  Success responses: 15
  Failure responses: 15
Local authentication statistics
  Total requests received: 5
  Success responses: 2
  Failure responses: 3
Securid authentication statistics
  Total requests received: 15
  Success responses: 3
  Failure responses: 12
```

 Copyright © 2011, Juniper Networks, Inc.

show network-access securid-node-secret-file

Syntax show network-access securid-node-secret-file

Release Information Command introduced in Release 9.1 of Junos OS.

Description Display the path to the node secret file for the SecurID authentication type.

Required Privilege Level view

Related Documentation

- configuration-file on page 17
- securid-server on page 44
- clear network-access securid-node-secret-file on page 1018

List of Sample Output show network-access securid-node-secret-file on page 1233

Output Fields Table 44 on page 1233 lists the output fields for the network-access securid-node-secret-filecommand. Output fields are listed in the approximate order in which they appear.

Table 44: show network-access securid-node-secret-file Output Fields

Field Name	Field Description
SecurID Server	Name of the SecurID authentication server.
Node Secret File	Path to the node secret file.

show network-access securid-node-secret-file

```
user@host> show network-access securid-node-secret-file
SecurID server node secret file:
SecurID Server       Node Secret File
ace-server1          /var/db/securid/ace-server1/node-secret
```

show poe controller

Syntax show poe controller

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display the status of the Power over Ethernet (PoE) controller.

Options **none**—Display general parameters of the PoE software module controller.

Required Privilege Level View

Output Fields Table 45 on page 1234 lists the output fields for the **show poe controller** command. Output fields are listed in the approximate order in which they appear.

Table 45: show poe controller Output Fields

Field name	Field Description
Controller-index	Identifies the controller.
Maximum-power	Specifies the maximum power that can be provided by the SRX Series device to PoE ports.
Power-consumption	Specifies the total amount of power allocated to the PoE ports.
Guard-band	Shows the guard band configured on the controller.
Management	Shows the power management mode.

show poe controller **user@host>show poe controller**

```
Controller  Maximum   Power              Guard band  Management
index       power     consumption
   0        150.0 W    0.0 W               0 W         Static
```


Copyright © 2011, Juniper Networks, Inc.

show poe interface

Syntax show poe interface <ge-fpc/pic/port>

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display the status of Power over Ethernet (PoE) ports.

Options **none**—Display the status of all PoE ports on the SRX Series device.

ge-fpc/pic/port— (Optional) Display the status of a specific PoE port on the SRX Series device.

Required Privilege Level View

Output Fields Table 46 on page 1235 lists the output fields for the **show poe interface** command. Output fields are listed in the approximate order in which they appear.

Table 46: show poe interface Output Fields

Field name	Field Description
PoE Interface	Specifies the interface name.
Admin Status	Specifies whether PoE capabilities are enabled or disabled.
Oper status	Specifies the operational status of the port.
Max-power	Specifies the maximum power configured on the port.
Priority	Specifies whether the port is high priority or low priority.
Power-consumption	Specifies how much power is being used by the port.
Class	Indicates the class of the powered device as defined by the IEEE 802 AF standard.

show poe interface

user@host>show poe interface

```
Interface Admin status Oper status Max power Priority Power consumption Class
    ge-0/0/0 Enabled      Searching   15.4W     Low      0.0W                0
    ge-0/0/1 Enabled      Powered-up  15.4W     High     6.6W                0
    ge-0/0/2 Disabled     Disabled    15.4W     Low      0.0W                0
    ge-0/0/3 Disabled     Disabled    15.4W     Low      0.0W                0
```

user@host>show poe interface ge-0/0/1

```
PoE interface status :
PoE interface                :  ge-0/0/1
Administrative status        : Enabled
Operational status           : Powered-up
Power limit on the interface : 15.4 W
```

```
Priority                     : High
Power consumed               : 6.6 W
Class of power device        :   0
```


Copyright © 2011, Juniper Networks, Inc.

show poe telemetries interface

Syntax show poe telemetries interface ge-fpc/pic/port all | x

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display a history of power consumption on the specified interface.

Options **ge-fpc/pic/port**—Display telemetries for the specified PoE interface.

all—Display all telemetries records for the specified PoE interface.

x—Display the specified number of telemetries records for the specified PoE interface.

Required Privilege Level View

Output Fields Table 47 on page 1237 lists the output fields for the **show poe telemetries interface** command. Output fields are listed in the approximate order in which they appear.

Table 47: show poe telemetries interface Output Fields

Field name	Field Description
Sl No	Number of the record for the specified port. The last record is the most is the most recent.
Timestamp	Time that the power-consumption data was gathered.
Power	Amount of power provided by the specified port at the time the data was gathered.
Voltage	Voltage on the specified port at the time the data was gathered.

show poe telemetries interface

user@host>show poe telemetries interface ge-0/0/1 all

```
Sl No    Timestamp                Power    Voltage
   1     Fri Jan 04 11:41:15 2009 6.6 W    47.2 V
   2     Fri Jan 04 11:40:15 2009 6.6 W    47.2 V
   3     Fri Jan 04 11:39:15 2009 6.6 W    47.2 V
   4     Fri Jan 04 11:38:15 2009 6.6 W    47.2 V
   5     Fri Jan 04 11:37:15 2009 6.6 W    47.2 V
   6     Fri Jan 04 11:36:15 2009 6.6 W    47.2 V
   7     Fri Jan 04 11:35:15 2009 6.6 W    47.2 V
   8     Fri Jan 04 11:34:15 2009 6.6 W    47.2 V
```

user@host>show poe telemetries interface ge-0/0/1 5

```
Sl No    Timestamp                Power    Voltage
   1     Fri Jan 04 11:47:15 2009 6.6 W    47.2 V
   2     Fri Jan 04 11:38:15 2009 6.6 W    47.2 V
   3     Fri Jan 04 11:29:15 2009 6.6 W    47.2 V
   4     Fri Jan 04 11:11:15 2009 6.6 W    47.2 V
```

Copyright © 2011, Juniper Networks, Inc.

```
5     Fri Jan 04 11:10:15 2009 6.6 W    47.2 V
```


Copyright © 2011, Juniper Networks, Inc.

show schedulers

Syntax

show schedulers
< **scheduler-name** *scheduler-name* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display information about security policy schedulers configured on the system. If a specific scheduler is identified, detailed information is displayed for that scheduler only.

Options

none—Display information on all configured schedulers.

scheduler-name *scheduler-name* —(Optional) Display information on a particular scheduler.

Required Privilege Level

view

Related Documentation

- **schedulers on page 264**

List of Sample Output

show schedulers on page 1239
show schedulers scheduler-name sch20 on page 1240

Output Fields

Table 48 on page 1239 lists the output fields for the **show schedulers** command. Output fields are listed in the approximate order in which they appear.

Table 48: show schedulers Output Fields

Field Name	Field Description
Scheduler name	Name of the scheduler.

State	Status of the scheduler:
	• **active**—The scheduler is associated with one or more policies. If active:
	  ◦ **Next deactivation**—Date and time when the policies with which the scheduler is associated are to be deactivated.
	• **inactive**—The scheduler is associated with one or more policies. If inactive:
	  ◦ **Next activation**—Date and time when the associated policies are to be activated.
	• **unused**—The scheduler is not associated with any policy, or it is past the stop date and no future activity is required.

show schedulers

```
user@host> show schedulers
Scheduler name: s1, State: unused
Scheduler name: sch1, State: inactive
  Next activation: Thu Feb 15 00:00:00 2007
Scheduler name: sch10, State: unused
Scheduler name: sch20, State: active
  Next deactivation: Thu Feb 15 00:00:00 2007
```

Copyright © 2011, Juniper Networks, Inc.

show schedulers scheduler-name sch20

```
user@host> show schedulers scheduler-name sch20
Scheduler name: sch20, State: active
  Next deactivation: Thu Feb 15 00:00:00 2007
```


Copyright © 2011, Juniper Networks, Inc.

show security alg h323 counters

Syntax

show security alg h323 counters
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display H.323 Application Layer Gateway (ALG) counters information.

Options

none—Display H.323 ALG counters. information.

node—(Optional) For chassis cluster configurations, display H.323 counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **h323 on page 483**
- **clear security alg h323 counters on page 1019**

List of Sample Output

show security alg h323 counters on page 1242

Output Fields

Table 49 on page 1241 lists the output fields for the **show security alg h323 counters** command. Output fields are listed in the approximate order in which they appear.

Table 49: show security alg h323 counters Output Fields

Field Name	Field Description
Packets received	Number of H.323 ALG packets received.
Packets dropped	Number of H.323 ALG packets dropped.
RAS message received	Number of incoming RAS (Endpoint Registration, Admission, and Status) messages per second per gatekeeper received and processed.
Q.931 message received	Counter for Q.931 message received.
H.245 message received	Counter for H.245 message received.

Copyright © 2011, Juniper Networks, Inc.

Table 49: show security alg h323 counters Output Fields *(continued)*

Field Name	Field Description
Number of calls	Total number of H.323 ALG calls. NOTE: This counter displays the number of call legs and may not display the exact number of voice calls that are active. For instance, for a single active voice call between two endpoints, this counter might display a value of **2**.
Number of active calls	Number of active H.323 ALG calls.
Decoding errors	Number of decoding errors.
Message flood dropped	Error counter for message flood dropped.
NAT errors	H.323 ALG Network Address Translation (NAT) errors.
Resource manager errors	H.323 ALG resource manager errors.

show security alg h323 counters

```
user@host> show security alg h323 counters
H.323 counters summary:
Packets received           :4060
Packets dropped            :24
RAS message received       :3690
Q.931 message received       :202
H.245 message received       :145
Number of calls        :25
Number of active calls       :0
H.323 Error Counters:
Decoding errors            :24
Message flood dropped       :0
NAT errors           :0
Resource manager errors       :0
H.323 Message Counters:
RRQ      : 431   RCF      :  49 ARQ  : 60  ACF      : 33
URQ      : 34   UCF      : 25 DRQ  : 55  DCF      : 44
oth RAS  : 2942  Setup    : 28 Alert    : 9 Connect    : 25
CallPrcd  : 18  Info    : 0  RelCmpl  : 39  Facility   : 14
Progress  : 0  Empty    : 65  OLC      : 20 OLC-ACK  :   20
oth H245  : 16
```


Copyright © 2011, Juniper Networks, Inc.

show security alg ike-esp-nat summary

Syntax show security alg ike-esp-nat summary

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display Application Layer Gateway (ALG) for IKE and ESP information summary.

Required Privilege Level view

Related Documentation

- clear security alg ike-esp-nat on page 1020

List of Sample Output show security alg ike-esp-nat summary on page 1243

show security alg ike-esp-nat summary

```
user@host> security alg ike-esp-nat summary
Initiator cookie: d5732d9b4114de1a
Responder cookie: 4776fe31164ef
Session-ID:       13
ALG state :       1
Timeout:          6292
Used IKE cookies: 0
Maximum IKE cookies: 2400
```

show security alg mgcp calls

Syntax

show security alg mgcp calls
<endpoint *endpoint-name* | node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) calls.

Options

none—Display all MGCP ALG calls.

endpoint *endpoint-name* —(Optional) Display information about the endpoints of each MGCP ALG call.

node—(Optional) For chassis cluster configurations, display MGCP calls on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **mgcp on page 575**
- **clear security alg mgcp calls on page 1021**

List of Sample Output

show security alg mgcp calls on page 1245
show security alg mgcp calls endpoint on page 1245

Output Fields

Table 50 on page 1244 lists the output fields for the **show security alg mgcp calls** command. Output fields are listed in the approximate order in which they appear.

Table 50: show security alg mgcp calls Output Fields

Field Name	Field Description
Connection ID	Connection identifier for MGCP ALG calls.
Local SDP	MGCP ALG call local owner IP address as per the Session Description Protocol (SDP).
Remote SDP	MGCP ALG call remote owner IP address as per the Session Description Protocol (SDP).
RM Group	Resource manager group ID.
Notified entity	The certificate authority (CA) currently controlling the gateway.

Copyright © 2011, Juniper Networks, Inc.

show security alg mgcp calls

```
user@host> show security alg mgcp calls
Endpoint@GW        Zone         Call ID                    RM Group
d001@101.50.10.1        Trust        10d55b81140e0f76          512
Connection Id> 0
Local SDP>   o: 101.50.10.1                x_o: 101.50.10.1
c: 101.50.10.1/32206          x_c: 101.50.10.1/32206
Remote SDP>  c: 3.3.3.5/16928              x_c: 3.3.3.5/16928
Endpoint@GW        Zone         Call ID                    RM Group
d001@3.3.3.5        Untrust      3a104e9b41a7c4c9          511
Connection Id> 0
Local SDP>   o: 3.3.3.5                    x_o: 3.3.3.5
c: 3.3.3.5/16928              x_c: 3.3.3.5/16928
Remote SDP>  c: 101.50.10.1/32206          x_c: 101.50.10.1/32206
```

show security alg mgcp calls endpoint

```
user@host> show security alg mgcp calls endpoint
Gateway: 101.50.10.1     Zone: Trust       IP: 101.50.10.1 -> 101.50.10.1
   Endpoint             Trans #  Call #   Notified Entity
   d001                 1        1        0.0.0.0/0->0.0.0.0/0
Gateway: 3.3.3.5      Zone: Untrust      IP: 3.3.3.5 -> 3.3.3.5
   Endpoint             Trans #  Call #   Notified Entity
   d001                 1        1        0.0.0.0/0->0.0.0.0/0
```

show security alg mgcp counters

Syntax

show security alg mgcp counters
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) counters information.

Options

none—Display MGCP ALG counters information.

node—(Optional) For chassis cluster configurations, display MGCP counters on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **mgcp on page 575**
- **clear security alg mgcp counters on page 1022**

List of Sample Output

show security alg mgcp counters on page 1247

Output Fields

Table 51 on page 1246 lists the output fields for the **show security alg mgcp counters** command. Output fields are listed in the approximate order in which they appear.

Table 51: show security alg mgcp counters Output Fields

Field Name	Field Description
Packets received	Number of MGCP ALG packets received.
Packets dropped	Number of MGCP ALG packets dropped.
Message received	Number of MGCP ALG messages received.
Number of connections	Number of MGCP ALG connections.
Number of active connections	Number of active MGCP ALG connections.
Number of calls	Number of MGCP ALG calls.

Copyright © 2011, Juniper Networks, Inc.

Table 51: show security alg mgcp counters Output Fields *(continued)*

Field Name	Field Description
Number of active calls	Number of MGCP ALG active calls.
Number of active transactions	Number of active transactions.
Number of re-transmission	Number of MGCP ALG retransmissions.
Unknown-method	MGCP ALG unknown method errors.
Decoding error	MGCP ALG decoding errors.
Transaction error	MGCP ALG transaction errors.
Call error	MGCP ALG counter errors.
Connection error	MGCP ALG connection errors.
Connection flood drop	MGCP ALG connection flood drop errors.
Message flood drop	MGCP ALG message flood drop error.
IP resolve error	MGCP ALG IP address resolution errors.
NAT error	MGCP ALG Network Address Translation (NAT) errors.
Resource manager error	MGCP ALG resource manager errors.

show security alg mgcp counters

```
user@host> show security alg mgcp counters
MGCP counters summary:
Packets received            :284
Packets dropped             :0
Message received            :284
Number of connections           :4
Number of active connections :3
Number of calls            :4
Number of active calls            :3
Number of transactions            :121
Number of active transactions:52
Number of re-transmission    :68
MGCP Error Counters:
Unknown-method            :0
Decoding error            :0
Transaction error            :0
Call error            :0
Connection error            :0
Connection flood drop            :0
Message flood drop            :0
IP resolve error            :0
NAT error            :0
Resource manager error            :0
MGCP Packet Counters:
```

```
CRCX   :4   MDCX     :9   DLCX     :2
AUEP   :1    AUCX     :0   NTFY     :43
RSIP   :79    EPCF     :0   RQNT     :51
000-199  :0     200-299  :95    300-999  :0
```


Copyright © 2011, Juniper Networks, Inc.

show security alg mgcp endpoints

Syntax

show security alg mgcp endpoints
< *endpoint name* >
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) endpoints.

Options

none—Display MGCP ALG endpoints information.

endpoint-name —(Optional) Display information about the specified MGCP ALG endpoint.

node—(Optional) For chassis cluster configurations, display MGCP endpoints on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **mgcp on page 575**

List of Sample Output

show security alg mgcp endpoints on page 1250
show security alg mgcp endpoints d001@100.100.100.152 on page 1250

Output Fields

Table 52 on page 1249 lists the output fields for the **show security alg mgcp endpoints** command. Output fields are listed in the approximate order in which they appear.

Table 52: show security alg mgcp endpoints Output Fields

Field Name	Field Description
Gateway	IP address of the gateway.
Zone	Gateway zone ID.
Endpoint	Endpoint name.
Trans #	Transaction ID.
Call #	Call ID.

Table 52: show security alg mgcp endpoints Output Fields *(continued)*

Field Name	Field Description
Notified entity	The certificate authority (CA) currently controlling the gateway.

show security alg mgcp endpoints

```
user@host> show security alg mgcp endpoints
Gateway: 100.100.100.152     Zone: z0             IP: 100.100.100.152 ->
100.100.100.152
  Endpoint          Trans #   Call #   Notified entity
  d001              3         1        0.0.0.0:0 -> 0.0.0.0:0
```

show security alg mgcp endpoints d001@100.100.100.152

```
user@host>  show security alg mgcp endpoints d001@100.100.100.152
Gateway: 100.100.100.152     Zone: z0             IP: 100.100.100.152 ->
100.100.100.152
  Endpoint          Trans #   Call #   Notified entity
  d001              12        2        0.0.0.0:0 -> 0.0.0.0:0
```


Copyright © 2011, Juniper Networks, Inc.

show security alg msrpc

Syntax

show security alg msrpc
<object-id-map> <node (*node-id* | all | local | primary)>

Release Information

Command updated in Release 10.1 of Junos OS.

Description

Display Microsoft (MS) remote procedure call (RPC) Application Layer Gateway (ALG) information.

Options

none—Display all MSRPC ID (UUID) to object ID (OID) table information.

object-id-map—(Optional) Display information from the MSRPC ID (UUID) to object ID (OID) table.

node—(Optional) For chassis cluster configurations, display MSRPC UUID-to-object-ID mapping information on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **msrpc on page 582**

List of Sample Output

show security alg msrpc object-id-map on page 1251

Output Fields

Table 53 on page 1251 lists the output fields for the **show security alg msrpc** command. Output fields are listed in the approximate order in which they appear.

Table 53: show security alg msrpc Output Fields

Field Name	Field Description
UUID	MS RPC ID.
OID	MS RPC object ID.

show security alg msrpc object-id-map

```
user@host> show security alg msrpc object-id-map
UUID                                    OID
1be617c0-31a5-11cf-a7d8-00805f48a135    0x80000020
e3514235-4b06-11d1-ab04-00c04fc2dcd2    0x80000002
67df7c70-0f04-11ce-b13f-00aa003bac6c    0x80000014
```

show security alg sccp calls

Syntax

show security alg sccp calls
< **brief** | **detail** | node (*node-id* | all | local | primary) >

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) calls.

Options

none | **brief**—Display brief call information.

detail—(Optional) Display detailed call information.

node—(Optional) For chassis cluster configurations, display SCCP calls on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sccp on page 696**
- **clear security alg sccp calls on page 1023**

List of Sample Output

show security alg sccp calls on page 1253
show security alg sccp calls detail on page 1253

Output Fields

Table 54 on page 1252 lists the output fields for the **show security alg sccp calls** command. Output fields are listed in the approximate order in which they appear.

Table 54: show security alg sccp calls Output Fields

Field Name	Field Description
Client IP address	IP address of the client.
Client zone	Client zone ID.
Call manager	IP address of the call manager.
Resource manager group	Resource manager group ID.

Copyright © 2011, Juniper Networks, Inc.

show security alg sccp calls

```
user@host> show security alg sccp calls
Client IP          Zone      CallManager       Conference ID  RM group
11.0.102.91        7         13.0.99.226       16789504       2047
12.0.102.96        8         13.0.99.226       16789505       2048
```

show security alg sccp calls detail

```
user@host> show security alg sccp calls detail
Client IP address: 11.0.102.91
Client zone: 7
CallManager IP: 13.0.99.226
Conference ID: 16789504
Resource manager group: 2048
SCCP channel information:
    Media transmit channel address (IP address/Port): 0.0.0.0:0
    Media transmit channel translated address (IP address/Port): 0.0.0.0:0
    Media transmit channel pass-through party ID (PPID): 0
    Media transmit channel resource ID: 0
    Media receive channel address (IP address/Port): 11.0.102.91:20060
    Media receive channel translated address (IP address/Port): 25.0.0.1:1032
    Media receive channel pass-through party ID (PPID): 16934451
    Media receive channel resource ID: 8185
    Multimedia transmit channel address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel pass-through party ID (PPID): 0
    Multimedia transmit channel resource ID: 0
    Multimedia receive channel address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel pass-through party ID (PPID): 0
    Multimedia receive channel resource ID: 0
Total number of calls = 1
```

Copyright © 2011, Juniper Networks, Inc.

show security alg sccp counters

Syntax

show security alg sccp counters
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

Options

none—Display all SCCP ALG counters.

node—(Optional) For chassis cluster configurations, display SCCP counters on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sccp on page 696**
- **clear security alg sccp counters on page 1024**

List of Sample Output

show security alg sccp counters on page 1255

Output Fields

Table 55 on page 1254 lists the output fields for the **show security alg sccp counters** command. Output fields are listed in the approximate order in which they appear.

Table 55: show security alg sccp counters Output Fields

Field Name	Field Description
Active client sessions	Number of active SCCP ALG client sessions.
Active calls	Number of active SCCP ALG calls.
Total calls	Total number of SCCP ALG calls.
Packets received	Number of SCCP ALG packets received.
PDUs processed	Number of SCCP ALG protocol data units (PDU) processed.
Current call rate	Number of calls per second.

Copyright © 2011, Juniper Networks, Inc.

Table 55: show security alg sccp counters Output Fields *(continued)*

Field Name	Field Description
Packets dropped	Number of packets dropped by the SCCP ALG.
Decode errors	Number of decoding errors.
Protocol errors	Number of protocol errors.
Address translation errors	Number of NAT errors.
Policy lookup errors	Number of errors occurring during policy lookups.
Unknown PDUs	Number of unknown protocol data units (PDUs).
Maximum calls exceed	Number of times the maximum number of calls was exceeded.
Maximum call rate exceed	Number of times the maximum call rate was exceeded.
Initialization errors	Number of call initialization errors.
Internal errors	Number of internal errors.
Nonspecific error	Number of nonspecific errors.

show security alg sccp counters

```
user@host> show security alg sccp counters
SCCP call statistics:
  Active client sessions         : 4
  Active calls                   : 2
  Total calls                    : 3
  Packets received               : 232
  PDUs processed                 : 232
  Current call rate              : 0
Error counters:
  Packets dropped                : 0
  Decode errors                  : 0
  Protocol errors                : 0
  Address translation errors     : 0
  Policy lookup errors           : 0
  Unknown PDUs                   : 0
  Maximum calls exceeded         : 0
  Maximum call rate exceeded     : 0
  Initialization errors          : 0
  Internal errors                : 0
  Nonspecific error              : 0
```

show security alg sip calls

Syntax

show security alg sip calls
<brief | detail | node (*node-id* | all | local | primary) >

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Session Initiation Protocols (SIP) Application Layer Gateway (ALG) calls.

Options

none | **brief**—Display brief call information.

detail—(Optional) Display detailed information about SIP ALG calls.

node—(Optional) For chassis cluster configurations, display SIP calls on a specific node (device) in the cluster.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sip on page 724**
- **clear security alg sip calls on page 1025**

List of Sample Output

show security alg sip calls on page 1256
show security alg sip calls detail on page 1257

Output Fields

Table 56 on page 1256 lists the output fields for the **show security alg sip calls** command. Output fields are listed in the approximate order in which they appear.

Table 56: show security alg sip calls Output Fields

Field Name	Field Description
UAS callid	Call Identifier for the SIP ALG user agent server.
State	State of the SIP ALG user agent server.

show security alg sip calls

```
user@host> show security alg sip calls
Total number of calls: 1
     Call ID  : 1-2468@20.0.0.174
   Method   : INVITE
```


Copyright © 2011, Juniper Networks, Inc.

show security alg sip calls detail

```
user@host> show security alg sip calls detail
Total number of calls: 1
       Call ID  : 1-2468@20.0.0.174
     Method   : INVITE
     State    : SETUP
     Group ID : 307
```

show security alg sip counters

Syntax

show security alg sip counters
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

Options

none—Display all SIP ALG counters.

node—(Optional) For chassis cluster configurations, display SIP counters on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sip on page 724**
- **clear security alg sip counters on page 1026**

List of Sample Output

show security alg sip counters on page 1260

Output Fields

Table 57 on page 1258 lists the output fields for the **show security alg sip counters** command. Output fields are listed in the approximate order in which they appear.

Table 57: show security alg sip counters Output Fields

Field Name	Field Description
INVITE	Number of INVITE requests sent. An INVITE request is sent to invite another user to participate in a session.
CANCEL	Number of CANCEL requests sent. A user can send a CANCEL request to cancel a pending INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE had sent a final response for the INVITE before it received the CANCEL
ACK	Number of ACK requests sent. The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request.
BYE	Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.

Copyright © 2011, Juniper Networks, Inc.

Table 57: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
RR header exceeded max	Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit.
REGISTER	Number of REGISTER requests sent. A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. A SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user.
OPTIONS	Number of OPTIONS requests sent. An OPTION request is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports.
INFO	Number of INFO requests sent. AN INFO message is used to communicate mid-session signaling information along the signaling path for the call.
MESSAGE	Number of MESSAGE requests sent. SIP messages consist of requests from a client to a server and responses to the requests from a server to a client with the purpose of establishing a session (or a call).
NOTIFY	Number of NOTIFY requests sent. NOTIFY requests are sent to inform subscribers of changes in state to which the subscriber has a subscription.
PRACK	Number of PRACK requests sent. The PRACK request plays the same role as ACK, but for provisional responses.
PUBLISH	Number of PUBLISH requests sent. The PUBLISH request used for publishing event state. PUBLISH is similar to REGISTER in that it allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user.
REFER	Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request.
SUBSCRIBE	Number of SUBSCRIBE requests sent. A SUBCRIBE request is used to request current state and state updates from a remote node.
UPDATE	Number of UPDATE requests sent. AN UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updates Session Description Protocol (SDP) information. The following fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route.
BENOTIFY	Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY.
SERVICE	Number of SERVICE requests sent. The SERVICE method used by a SIP client to request a service of a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user which is performing the service.
OTHER	Number of OTHER requests sent.
Total Pkt-in	Number of SIP ALG total packets received.

Copyright © 2011, Juniper Networks, Inc.

Table 57: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
Total Pkt dropped on error	Number of SIP ALG total packets dropped while transmission and retransmission of messages.
Call error	Number of SIP ALG call errors.
IP resolve error	Number of SIP ALG IP address resolution errors.
NAT error	Number of SIP ALG NAT errors.
Resource manager error	Number of SIP ALG resource manager errors.
Contact header exceeded max	Number of times the SIP ALG contact headers exceeded the maximum limit.
Invite Dropped due to call limit	Number of SIP ALG invite dropped due to call limits.
SIP msg not processed by stack	Number of SIP ALG stack errors.
SIP msg not processed by alg	Number of SIP ALG messages not processed by ALGs.
SIP unknown method dropped	Number of SIP ALG unknown method errors.
Decoding error	Number of SIP ALG decoding errors.
Request for disconnected call	Number of SIP ALG calls disconnected.
Request out of state	Number of SIP ALG messages out of state errors.

show security alg sip counters

```
user@host> show security alg sip counters
SIP message counters(T:Transmit, RT:Retransmit):
   Method      T    1xx    2xx    3xx   4xx    5xx    6xx
               RT   RT     RT     RT    RT     RT     RT
   INVITE      4    4      3      0     0      0      0
               0    0      0      0     0      0      0
   CANCEL      0    0      0      0     0      0      0
               0    0      0      0     0      0      0
      ACK      3    0      0      0     0      0      0
               0    0      0      0     0      0      0
      BYE      3    0      3      0     0      0      0
               0    0      0      0     0      0      0
 REGISTER      7    0      7      0     0      0      0
               0    0      0      0     0      0      0
  OPTIONS      0    0      0      0     0      0      0
               0    0      0      0     0      0      0
     INFO      0    0      0      0     0      0      0
               0    0      0      0     0      0      0
  MESSAGE      0    0      0      0     0      0      0
               0    0      0      0     0      0      0
   NOTIFY      0    0      0      0     0      0      0
               0    0      0      0     0      0      0
    PRACK      0    0      0      0     0      0      0
```


Copyright © 2011, Juniper Networks, Inc.

```
                0    0     0     0    0     0     0
  PUBLISH       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
    REFER       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
SUBSCRIBE       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
   UPDATE       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
 BENOTIFY       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
  SERVICE       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
    OTHER       0    0     0     0    0     0     0
                0    0     0     0    0     0     0
SIP Error Counters:
Total Pkt-in                        :34
Total Pkt dropped on error          :0
Call error                          :0
IP resolve error                    :0
NAT error                           :0
Resource manager error              :0
RR header exceeded max              :0
Contact header exceeded max         :0
Call Dropped due to limit                  : 0
SIP stack error                                     : 0
SIP decode error                                 : 0
SIP unknown method error              : 0
RTO message sent                           : 0
RTO message received                   : 0
RTO buffer allocation failure            : 0
RTO buffer transmit failure              : 0
RTO send processing error            : 0
RTO receive processing error         : 0
RTO receive invalid length               : 0
RTO receive call process error       : 0
RTO receive call allocation error    : 0
RTO receive call register error        : 0
RTO receive invalid status error     : 0
```

show security alg sip rate

Syntax

show security alg sip rate
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display rate information for Session Initiation Protocol (SIP) Application Layer Protocol (ALG) messages.

Options

none—Display all SIP ALG rate information.

node—(Optional) For chassis cluster configurations, display SIP rate on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sip on page 724**

List of Sample Output

show security alg sip rate on page 1262

Output Fields

Table 58 on page 1262 lists the output fields for the **show security alg sip rate** command. Output fields are listed in the approximate order in which they appear.

Table 58: show security alg sip rate Output Fields

Field Name	Field Description
CPU ticks	SIP ALG CPU ticks per microsecond.
Time taken	Time, in microseconds, that the last SIP ALG message needed to transit the network.
Total time	Total time, in microseconds, during an interval of less than 10 minutes for the specified number of SIP ALG messages to transit the network.
Rate	Number of SIP ALG messages per second transiting the network.

show security alg sip rate

```
user@host> show security alg sip rate
CPU ticks per us is 166
Time taken for the last message is 1103 us
```


Copyright © 2011, Juniper Networks, Inc.

```
Total time taken for 3124 messages is 6221482 us (in less than 10 minutes)
Rate: 502 messages/second
```

show security alg sip transactions

Syntax

show security alg sip transactions
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about Session Initiation Protocol (SIP) Application Layer Gateway (ALG) transactions.

Options

none—Display all SIP ALG transactions.

node—(Optional) For chassis cluster configurations, display SIP transactions on a specific node (device) in the cluster.

node-id—Identification number of the node. It can be 0 or 1.

all—Display information about all nodes.

local—Display information about the local node.

primary—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **sip on page 724**

List of Sample Output

show security alg sip transactions on page 1264

Output Fields

Table 59 on page 1264 lists the output fields for the **show security alg sip transaction** command. Output fields are listed in the approximate order in which they appear.

Table 59: show security alg sip transactions Output Fields

Field Name	Field Description
UAS	SIP ALG User Agent Server transaction name.
UAC	ALG SIP User Agent Client transaction name.

show security alg sip transactions

```
user@host> show security alg sip transactions
Total number of transactions: 1
Transaction Name        Method    CSeq       State         Timeout    VIA RSC ID
UAS:tsx0x4b06ddf4          BYE    101     Proceeding            -1        -
UAC:tsx0x4b06f610          BYE    101        Calling            27     8185
```


Copyright © 2011, Juniper Networks, Inc.

show security alg status

Syntax **show security alg status**

Release Information Command modified in Release 9.5 of Junos OS

Description Display the status (enabled/disabled) of the supported Application Layer Gateway (ALG) transactions.

This command is supported on SRX Series and J Series devices. The following list describes the default status on each of these devices:

- SRX3000 and SRX5000 line devices—FTP ALGs and TFTP ALGs are enabled by default. All other ALGs are disabled.
- SRX100, SRX210, SRX240, and SRX650 devices—All supported ALGs are enabled by default.
- J Series devices—All supported ALGs are enabled by default.

For complete information about which ALGs are supported on which devices, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

Options none—Display status of all supported ALGs.

Required Privilege Level view

Output Fields The following list describes the output fields for the **show security alg status** command. Output fields are listed in the approximate order in which they appear.

- **DNS**—Domain Name Server
- **FTP**—File Transfer Protocol
- **H323**—H.323 protocol
- **MGCP**—Media Gateway Control Protocol
- **MSRPC**—Microsoft remote procedure call
- **PPTP**—Point-to-Point Tunneling Protocol
- **RSH**—UNIX remote shell services
- **RTSP**—Real-Time Streaming Protocol
- **SCCP**—Skinny Client Control Protocol
- **SIP**—Session Initiation Protocol
- **SQL**—Oracle SQL
- **SUNRPC**—Sun Microsystems remote procedure call

Copyright © 2011, Juniper Networks, Inc.

- **TALK**—TALK program
- **TFTP**—Trivial File Transfer Protocol

show security alg status

```
user@host> show security alg status
ALG Status :

  DNS      : Enabled

  FTP      : Enabled

  H323     : Disabled

  MGCP     : Disabled

  MSRPC    : Enabled

  PPTP     : Enabled

  RSH      : Enabled

  RTSP     : Enabled

  SCCP     : Disabled

  SIP      : Disabled

  SQL      : Enabled

  SUNRPC   : Enabled

  TALK     : Enabled

  TFTP     : Enabled
```


Copyright © 2011, Juniper Networks, Inc.

show security application-firewall rule-set

Syntax

show security application-firewall rule-set
<rule-set-name>
all

Release Information

Command introduced in Release 11.1 of Junos OS.

Description

Display information about the specified rule set defined in the application firewall.

Options

rule-set-name—Name of the rule set.

all—Display information about all the application firewall rule sets.

Required Privilege Level

view

Related Documentation

clear security application-firewall rule-set statistics on page 1027

List of Sample Output

show security application-firewall rule-set my_ruleset1 on page 1268
show security application-firewall rule-set all on page 1268

Output Fields

Table 60 on page 1267 lists the output fields for the **show security application-firewall rule-set** command. Output fields are listed in the approximate order in which they appear.

Table 60: show security application-firewall rule-set Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.

Rule	Name of the rule
	• **Dynamic applications**—Name of the applications.
	• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ◦ **permit**
	  ◦ **deny**
	• **Number of sessions matched**—Number of sessions matched with the application firewall rule.

Default rule	The default rule applied when the identified application is not specified in any rules of the rule set. • **Number of sessions matched**—Number of sessions matched with the application firewall default rule.
Number of sessions with appid pending	Number of sessions that are pending with the application ID processing

Copyright © 2011, Juniper Networks, Inc.

show security application-firewall rule-set my_ruleset1

```
user@host>show security application-firewall rule-set my_ruleset1
Rule-set: my_ruleset1
           Rule: rule1
               Dynamic Applications: junos:facebook, junos:messenger
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 2
```

show security application-firewall rule-set all

```
user@host>  show security application-firewall rule-set all
Rule-set: my_ruleset1
           Rule: rule1
               Dynamic Applications: junos:facebook, junos:messenger
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 5
        Rule-set: my_ruleset2
           Rule: rule2
               Dynamic Applications: junos: http
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security application-tracking counters

Syntax show security application-tracking counters

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the status of AppTrack counters.

Required Privilege Level view

Output Fields Table 61 on page 1269 lists the output fields for the **show security application-tracking counters** command. Output fields are listed in the approximate order in which they appear.

Table 61: show security application-tracking counters

Field Name	Field Description
Session create messages	The number of log messages generated when a session was created.
Session close messages	The number of log messages generated when a session was closed.
Session volume updates	The number of log messages generated when an update interval was exceeded.
Failed messages	The number of messages that were not generated due to memory or session constraints.

show security application-tracking counters

```
user@host> show security application-tracking counters
AVT counters:                        Value
 Session create messages               0
 Session close messages                0
 Session volume updates                0
 Failed messages                       0
```

show security datapath-debug capture

Syntax show security datapath-debug capture

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display details of the data path debugging capture file.

Required Privilege Level view

Related Documentation

- **show security datapath-debug counter on page 1271**

List of Sample Output **show security datapath—debug capture on page 1270**

Output Fields Output fields are listed in the approximate order in which they appear.

show security datapath—debug capture

```
user@host> show security datapath-debug capture
Packet 1, len 120: (C0/F0/P0/SEQ:71:lbt)
91 00 00 47 11 00 10 00 9a 14 00 19 03 00 00 00
00 00 00 00 00 01 00 47 10 00 00 00 00 00 00 00
00 1f 12 f8 dd 29 00 21 59 84 f4 01 81 00 02 1e
08 00 45 60 01 f4 00 00 00 00 3f 06 73 9f 01 01
01 02 03 01 01 02 d4 31 d4 31 00 00 00 00 00 00
00 00 50 02 00 00 ff ad 00 00 00 00
Packet 2, len 120: (C0/F0/P0/SEQ:71:lbt)
90 00 00 47 04 00 00 00 00 00 00 00 02 02 00 47
10 00 00 00 00 00 00 00 50 00 a6 1c 00 00 00 00
00 00 00 0a 00 00 00 00 00 00 09 d9 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 1f 12 f8
dd 29 00 21 59 84 f4 01 81 00 02 1e
```


Copyright © 2011, Juniper Networks, Inc.

show security datapath-debug counter

Syntax show security datapath-debug counter

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display details of the data path debugging counter.

Required Privilege Level view

Related Documentation

- **show security datapath-debug capture on page 1270**

List of Sample Output **show security datapath-debug counter on page 1271**

Output Fields Output fields are listed in the approximate order in which they appear.

show security datapath-debug counter

```
user@host> show security datapath-debug counter
Datapath debug counters
Packet Filter 1:
np-ingress
Chassis 0 FPC 4 : 1
np-ingress
Chassis 0 FPC 3 : 0
np-egress
Chassis 0 FPC 4 : 1
np-egress
Chassis 0 FPC 3 : 0
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 2
pot
Chassis 0 FPC 0 PIC 1: 0
pot
```

Copyright © 2011, Juniper Networks, Inc.

show security dynamic-policies

Syntax show security dynamic-policies [detail] [from-zone *zone*] [scope-id *id*] [to-zone *zone*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display dynamic policies downloaded on the group member.

Options none—Display basic information about all policies installed on the group member.

detail—(Optional) Display a detailed view of all of the policies installed on the group member.

from-zone—(Optional) Display information about the policies installed on the group member for the specified source zone.

scope-id—(Optional) Display information about the policies installed on the group member for the specified policy identifier.

to-zone—(Optional) Display information about the policies installed on the group member for the specified destination zone.

Required Privilege Level view

Related Documentation

- **show security policies on page 1540**

Output Fields Table 62 on page 1272 lists the output fields for the **show security dynamic-policies** command. Output fields are listed in the approximate order in which they appear.

Table 62: show security dynamic-policies Output Fields

Field Name	Field Description
Policy	Name of the applicable Policy.
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	An internal number associated with the policy.
Scope Policy	Policy identifier.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.

Copyright © 2011, Juniper Networks, Inc.

Table 62: show security dynamic-policies Output Fields *(continued)*

Field Name	Field Description
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. (In this case, only the names are given, not their IP addresses.) For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
Application	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The IP protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0. • **Inactivity timeout**: Elapse time without activity after which the application is terminated. • **Source port range**: The low-high source port range for the session application. • **Destination port range**: The low-high destination port range for the session application.
action-type	Must be permit.
Policy Type	Must be dynamic.
From zone	Name of the source zone.
To zone	Name of the destination zone.
Tunnel	Tunnel name, type (IPsec), and index number.

show security dynamic-policies

```
user@host> show security dynamic-policies
Policy: policy_forward-0001, State: enabled, Index: 1048580, Scope Policy: 4
  Sequence number: 1
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
    Applications: Unknown
action-type: permit, tunnel:
Policy: policy_forward-0002, State: enabled, Index: 2097156, Scope Policy: 4
  Sequence number: 2
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
    Applications: Unknown
action-type: permit, tunnel:
```

show security dynamic-policies detail

```
user@host> show security dynamic-policies detail
Policy: policy_forward-0001, action-type: permit, State: enabled, Index:
1048580,AI: disabled, Scope Policy: 4
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Host, To zone: untrust
```

```
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [23-23]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1001
Policy: policy_backward-0001, action-type: permit, State: enabled, Index:
1048582,AI: disabled, Scope Policy: 6
  Policy Type: Dynamic
  Sequence number: 1
  From zone: untrust, To zone: Host
  Source addresses:20.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1003
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1005
Policy: policy_external-0001, action-type: permit, State: enabled, Index:
1048584,AI: disabled, Scope Policy: 8
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: untrust
  Source addresses:192.168.1.0/24
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1006
Policy: policy_forward-0002, action-type: permit, State: enabled, Index:
2097156,AI: disabled, Scope Policy: 4
  Policy Type: Dynamic
  Sequence number: 2
  From zone: Host, To zone: untrust
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1002
Policy: policy_backward-0002, action-type: permit, State: enabled, Index:
2097158,AI: disabled, Scope Policy: 6
  Policy Type: Dynamic
  Sequence number: 2
  From zone: untrust, To zone: Host
  Source addresses:20.10.10.0/16
```

 Copyright © 2011, Juniper Networks, Inc.

```
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [23-23]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1004
```

show security dynamic-policies from-zone Internal

```
user@host> show security dynamic-policies from-zone Internal
Policy: policy_internal-0001, State: enabled, Index: 1048583, Scope Policy: 7
  Sequence number: 1
    Applications: Unknown
action-type: permit, tunnel:
Policy: policy_external-0001, State: enabled, Index: 1048584, Scope Policy: 8
  Sequence number: 1
    Applications: Unknown
action-type: permit, tunnel:
```

show security dynamic-policies scope-id 8 from-zone Internal

```
user@host> show security dynamic-policies scope-id 8 from-zone Internal
Policy: policy_external-0001, State: enabled, Index: 1048584, Scope Policy: 8
  Sequence number: 1
    Applications: Unknown
action-type: permit, tunnel:
```

show security dynamic-policies detail from-zone Internal

```
user@host> show security dynamic-policies detail from-zone Internal
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1005
Policy: policy_external-0001, action-type: permit, State: enabled, Index:
1048584,AI: disabled, Scope Policy: 8
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: untrust
  Source addresses:192.168.1.0/24
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1006
```

show security dynamic-policies detail from-zone Internal to-zone Host

```
user@host> show security dynamic-policies detail from-zone Internal to-zone Host
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
```

```
    Destination port range: [80-80]
Tunnel: Test Tunnel, Type: IPSec, Index: 1005
```


Copyright © 2011, Juniper Networks, Inc.

show security dynamic-vpn client version

Syntax show security dynamic-vpn client version

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display the client software version.

Required Privilege Level view

Sample Output

```
user@host> show security dynamic-vpn client version
Juniper Access Manager version: 1.1.0.4165
```

show security dynamic-vpn users

Syntax show security dynamic-vpn users

Release Information Command introduced in Release 10.0 of Junos OS.

Description This command shows relevant user information.

Required Privilege Level view

Output Fields Table 63 on page 1278 lists the output fields for the **show security dynamic-vpn users** command. Output fields are listed in the approximate order in which they appear.

Table 63: show security dynamic-vpn users Output Fields

Field Name	Field Description
User	Username.
Number of connections	Number of connections currently active.
Remote IP	IP address of the client.
IPsec VPN	Name of the IPsec VPN.
IKE gateway	Name of the IKE gateway.
IKE ID	IKE ID configured for the client.
Status	Status of the connection.

Sample Output

```
user@host> show security dynamic-vpn users
User: sally , Number of connections: 1
    Remote IP: 10.150.73.11

    IPSEC VPN: client6vpn

    IKE gateway: ikegateway6

    IKE ID   : bob6.juniper.net

    Status: CONNECTED
```


Copyright © 2011, Juniper Networks, Inc.

show security dynamic-vpn users terse

Syntax show security dynamic-vpn users terse

Release Information This command introduced in Release 10.0 of Junos OS.

Description Display all relevant user information.

Required Privilege Level view

Output Fields Table 64 on page 1279 lists the output fields for the **show security dynamic-vpn users terse** command. Output fields are listed in the approximate order in which they appear.

Table 64: show security dynamic-vpn users terse Output Fields

Field Name	Field Description
User	Username.
Remote IP	IP address of the client.
IKE ID	IKE ID configured for the client.
Status	Status of the connection.
Client Config Name	Name of the client configuration.
Time Established	Time that the user connection was established.

Sample Output

```
user@host> show security dynamic-vpn users terse
User  Remote IP    IKE ID             Status   Client Config Name   Time
Established
sally 10.150.73.11 bob6.juniper.net  CONNECTED   cfg6                Tue Jul 21
10:11:50 2009
```

show security firewall-authentication history

Syntax

show security firewall-authentication history
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display security firewall authentication history information.

Options

none—Display history of firewall authentication information.

node—(Optional) For chassis cluster configurations, display all firewall authentication history on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication history on page 1031**

List of Sample Output

show security firewall-authentication history on page 1281
show security firewall-authentication history node all on page 1281

Output Fields

Table 65 on page 1280 lists the output fields for the **show security firewall-authentication history** command. Output fields are listed in the approximate order in which they appear.

Table 65: show security firewall-authentication history Output Fields

Field Name	Field Description
Authentications	Number of authentications.
Id	Identification number.
Source IP	IP address of the authentication source.
Date	Authentication date.
Time	Authentication time.
Duration	Authentication duration.

Copyright © 2011, Juniper Networks, Inc.

Table 65: show security firewall-authentication history Output Fields *(continued)*

Field Name	Field Description
Status	Authentication status success or failure.
User	Name of the user.

show security firewall-authentication history

```
user@host> show security firewall-authentication history
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 211.0.0.6       2007-04-03 11:43:06 00:00:45   Success  hello
```

show security firewall-authentication history node all

```
user@host> show security firewall-authentication history node all
node0:
--------------------------------------------------------------------------
History of firewall authentication data:
Authentications: 2
Id Source Ip       Date       Time     Duration   Status   User
1 100.0.0.1       2008-01-04 12:00:10 0:05:49    Success  local1
2 100.0.0.1       2008-01-04 14:36:52 0:01:03    Success  local1
node1:
--------------------------------------------------------------------------
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 100.0.0.1       2008-01-04 14:59:43 1193046:06: Success local1
```

Copyright © 2011, Juniper Networks, Inc.

show security firewall-authentication history address

Syntax

show security firewall-authentication history address *ip-address*
<node (*node-id* **| all | local | primary)>**

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display security firewall authentication history for this source IP address.

Options

address *ip-address* —IP address of the authentication source.

none—Display all firewall authentication history for this address.

node—(Optional) For chassis cluster configurations, display firewall authentication history for this address on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication history address on page 1032**

List of Sample Output

show security firewall-authentication history address 4.4.4.2 on page 1283
show security firewall-authentication history address 100.0.0.1 node local on page 1283

Output Fields

Table 66 on page 1282 lists the output fields for the **show security firewall-authentication history address** command. Output fields are listed in the approximate order in which they appear.

Table 66: show security firewall-authentication history address Output Fields

Field Name	Field Description
Username	User ID.
Source IP	IP address of the authentication source.
Authentication state	Status of authentication (success or failure).
Authentication method	Path chosen for authentication.
Access start date	Date when user authenticated.

Copyright © 2011, Juniper Networks, Inc.

Table 66: show security firewall-authentication history address Output Fields *(continued)*

Field Name	Field Description
Access start time	Time when user authenticated.
Duration of user access	Time duration of the accessing firewall.
Policy name	Name of the policy.
Source zone	User traffic received from the zone.
Destination zone	User traffic destined to the zone.
Access profile	Name of profile used for authentication.
Bytes sent by this user	Number of bytes sent by the user.
Bytes received by this user	Number of bytes received by the user.

show security firewall-authentication history address 4.4.4.2

```
user@host> show security firewall-authentication history address 4.4.4.2
Username: u1
Source IP: 4.4.4.2
Authentication state: Success
Authentication method: Pass-through using HTTP
Access start date: 2007-09-12
Access start time: 15:33:29
Duration of user access: 0:00:48
Policy name: Z1-Z2
Source zone: Z1
Destination zone: Z2
Access profile: profile-local
Bytes sent by this user: 0
Bytes received by this user: 449
```

show security firewall-authentication history address 100.0.0.1 node local

```
user@host> show security firewall-authentication history address 100.0.0.1 node local
node0:
--------------------------------------------------------------------------
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
Access start time: 12:00:10
Duration of user access: 0:05:49
Policy name: POL1
Source zone: z1
Destination zone: z2
Access profile: p1
Bytes sent by this user: 0
Bytes received by this user: 0
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
```

```
Access start time: 14:36:52
Duration of user access: 0:01:03
Policy name: POL1
Source zone: z1
Destination zone: z2
Access profile: p1
Bytes sent by this user: 2178
Bytes received by this user: 4172
```


Copyright © 2011, Juniper Networks, Inc.

show security firewall-authentication history identifier

Syntax

show security firewall-authentication history identifier ***identifier***
<node (***node-id*** | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display security firewall authentication history information for the authentication with this identifier.

Options

identifier ***identifier***—Identifying number of the authentication process.

none—Display all firewall authentication history information for the authentication with this identifier.

node—(Optional) For chassis cluster configurations, display firewall authentication history on a specific node for the authentication with this identifier.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication history identifier on page 1033**

List of Sample Output

show security firewall-authentication history identifier 1 on page 1286
show security firewall-authentication identifier 1 node primary on page 1286

Output Fields

Table 67 on page 1285 lists the output fields for the **show security firewall-authentication history identifier** command. Output fields are listed in the approximate order in which they appear.

Table 67: show security firewall-authentication history identifier Output Fields

Field Name	Field Description
Username	User ID.
Source IP	IP address of the authentication source.
Authentication state	Status of authentication (success or failure).
Authentication method	Path chosen for authentication.

Copyright © 2011, Juniper Networks, Inc.

Table 67: show security firewall-authentication history identifier Output Fields *(continued)*

Field Name	Field Description
Access start date	Date when user authenticated.
Access start time	Time when user authenticated.
Duration of user access	Time duration of the accessing firewall.
Policy index	Identification number of the policy.
Policy name	Name of the policy.
Source zone	User traffic received from the zone.
Destination zone	User traffic destined to the zone.
Access profile	Name of profile used for authentication.
Bytes sent by this user	Number of bytes sent by the user.
Bytes received by this user	Number of bytes received by the user.
Client-groups	Name of the client group.

show security firewall-authentication history identifier 1

```
user@host> show security firewall-authentication history identifier 1
Username: hello
Source IP: 211.0.0.6
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2007-04-03
Access start time: 11:43:06
Duration of user access: 00:00:45
Policy index: 4
Source zone: z2
Destination zone: z1
Access profile: profile1
Bytes sent by this user: 0
Bytes received by this user: 1050
Client-groups: Sunnyvale Bangalore
```

show security firewall-authentication identifier 1 node primary

```
user@host> show security firewall-authentication history identifier 1 node primary
node0:
--------------------------------------------------------------------------
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
Access start time: 12:00:10
Duration of user access: 0:05:49
Policy name: POL1
Source zone: z1
Destination zone: z2
```


Copyright © 2011, Juniper Networks, Inc.

```
Access profile: p1
Bytes sent by this user: 0
Bytes received by this user: 0
```

show security firewall-authentication users

Syntax

show security firewall-authentication users
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display firewall authentication details about all users.

Options

none—Display details about all firewall authentication users.

node—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication users on page 1034**

List of Sample Output

show security firewall-authentication users on page 1289
show security firewall-authentication users node 0 on page 1289
show security firewall-authentication users node all on page 1289

Output Fields

Table 68 on page 1288 lists the output fields for the **show security firewall-authentication users** command. Output fields are listed in the approximate order in which they appear.

Table 68: show security firewall-authentication users Output Fields

Field Name	Field Description
Total users in table	Gives count of how many entries/users the command will display.
Id	Identification number.
Source IP	IP address of the authentication source.
Src zone	User traffic received from the zone.
Dst zone	User traffic destined to the zone.
Profile	Name of profile used for authentication.

Copyright © 2011, Juniper Networks, Inc.

Table 68: show security firewall-authentication users Output Fields *(continued)*

Field Name	Field Description
Age	Idle timeout for the user.
Status	Authentication status success or failure.
User	Name of the user.

show security firewall-authentication users

```
user@host> show security firewall-authentication users
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           1 10.0.0.1        z1       z2       p1           0 Success  local1
```

show security firewall-authentication users node 0

```
user@host> show security firewall-authentication users node 0
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User

           3 100.0.0.1       z1       z2       p1           1 Success  local1
```

show security firewall-authentication users node all

```
user@host> show security firewall-authentication users node all
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           3 100.0.0.1       z1       z2       p1           1 Success  local1

node1:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           2 100.0.0.1       z1       z2       p1           1 Success  local1
```

show security firewall-authentication users address

Syntax

show security firewall-authentication users address ***ip-address***
<node (***node-id*** | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display information about the users at the specified IP address that are currently authenticated.

Options

address ***ip-address*****—**IP address of the authentication source.

none—Display all the firewall authentication information for users at this IP address.

node—(Optional) For chassis cluster configurations, display user firewall authentication entries on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication users address on page 1035**

List of Sample Output

show security firewall-authentication users address 211.0.0.6 on page 1291
show security firewall-authentication users address 100.0.0.1 node local on page 1291

Output Fields

Table 69 on page 1290 lists the output fields for the **show security firewall-authentication users address** command. Output fields are listed in the approximate order in which they appear.

Table 69: show security firewall-authentication users address Output Fields

Field Name	Field Description
Username	User ID.
Source IP	IP address of the authentication source.
Authentication state	Status of authentication (success or failure).
Authentication method	Path chosen for authentication.
Access time remaining	Duration for which the connection exists.

Copyright © 2011, Juniper Networks, Inc.

Table 69: show security firewall-authentication users address Output Fields *(continued)*

Field Name	Field Description
Source zone	User traffic received from the zone.
Destination zone	User traffic destined to the zone.
Policy index	Identification number of the policy.
Policy name	Name of the policy.
Access profile	Name of profile used for authentication.
Interface Name	Name of the interface.
Bytes sent by this user	Number of bytes sent by the user.
Bytes received by this user	Number of bytes received by the user.
Client-groups	Name of the client group.

show security firewall-authentication users address 211.0.0.6

```
user@host>show security firewall-authentication users address 211.0.0.6
Username: hello
Source IP: 211.0.0.6
Authentication state: Success
Authentication method: Pass-through using Telnet
Access time remaining: 0
Source zone: z2
Destination zone: z1
Policy index: 5
Access profile: profile1
Interface Name: ge-0/0/2.0
Bytes sent by this user: 0
Bytes received by this user: 0
Client-groups: Sunnyvale Bangalore
```

show security firewall-authentication users address 100.0.0.1 node local

```
user@host> show security firewall-authentication users address 100.0.0.1 node local
node0:
--------------------------------------------------------------------------
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Age: 2
Access time remaining: 4
Source zone: z1
Destination zone: z2
Policy name: POL1
Access profile: p1
Interface Name: reth1.0
Bytes sent by this user: 614
Bytes received by this user: 1880
```

show security firewall-authentication users identifier

Syntax

show security firewall-authentication users identifier ***identifier***
<node (***node-id*** | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display firewall authentication details about the user with this identification number.

Options

identifier ***identifier***—Identification number of the user for which to display authentication details.

node—(Optional) For chassis cluster configurations, display the firewall authentication details security firewall authentication entry on a specific node (device) in the cluster for the user with this identification number.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **firewall-authentication (Security) on page 453**
- **clear security firewall-authentication users identifier on page 1036**

List of Sample Output

show security firewall-authentication users identifier 3 on page 1293
show security firewall-authentication users identifier 3 node primary on page 1293

Output Fields

Table 70 on page 1292 lists the output fields for the **show security firewall-authentication users identifier** command. Output fields are listed in the approximate order in which they appear.

Table 70: show security firewall-authentication users identifier Output Fields

Field Name	Field Description
Username	User ID.
Source IP	IP address of the authentication source.
Authentication state	Status of authentication (success or failure).
Authentication method	Path chosen for authentication.
Age	Idle timeout for the user.

Copyright © 2011, Juniper Networks, Inc.

Table 70: show security firewall-authentication users identifier Output Fields *(continued)*

Field Name	Field Description
Access time remaining	Duration for which the connection exists.
Source zone	User traffic received from the zone.
Destination Zone	User traffic destined to the zone.
Policy Name	Name of the policy.
Access profile	Name of profile used for authentication.
Interface Name	Name of the interface
Bytes sent by this user	Number of bytes sent by the user.
Bytes received by this user	Number of bytes received by the user.

show security firewall-authentication users identifier 3

```
user@host> show security firewall-authentication users identifier 3
Username: u1
Source IP: 4.4.4.2
Authentication state: Success
Authentication method: Pass-through using HTTP
Age: 1
Access time remaining: 254
Source zone: Z1
Destination zone: Z2
Policy name: Z1-Z2
Access profile: profile-local
Interface Name: ge-0/0/1.0
Bytes sent by this user: 0
Bytes received by this user: 449
```

show security firewall-authentication users identifier 3 node primary

```
user@host> show security firewall-authentication users identifier 3 node primary
node0:
--------------------------------------------------------------------------
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Age: 1
Access time remaining: 5
Source zone: z1
Destination zone: z2
Policy name: POL1
Access profile: p1
Interface Name: reth1.0
Bytes sent by this user: 614
Bytes received by this user: 1880
```

show security flow cp-session

Syntax

show security flow cp-session
[<filter>] [summary | terse]

Release Information

Command introduced in Release 10.2 of Junos OS.

Description

Display central point session-related flow information.

Options

destination-port—Destination port

destination-prefix—Destination prefix

family—Display session by family.

protocol—IP protocol number

source-port—Source port

source-prefix—Source IP prefix or address

summary | terse—Display the specified level of output.

Required Privilege Level

view

List of Sample Output

show security flow cp-session summary on page 1295
show security flow cp-session terse on page 1295

Output Fields

Table 71 on page 1294 lists the output fields for the **show security flow cp-session** command. Output fields are listed in the approximate order in which they appear.

Table 71: show security flow cp-session Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Maximum sessions	Number of maximum central point sessions.
Maximum inet6 sessions	Number of maximum inet6 central point sessions.
Session ID	Number that identifies the session. Use this ID to get more information about the session.

Copyright © 2011, Juniper Networks, Inc.

Table 71: show security flow cp-session Output Fields *(continued)*

Field Name	Field Description
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

show security flow cp-session summary

```
root> show security flow cp-session summary
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
Maximum sessions: 10485760
Maximum inet6 sessions: 5242880
```

show security flow cp-session terse

```
root> show security flow cp-session terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session destination-port

Syntax **show security flow cp-session destination-port *destination-port-number* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session-related flow information for the specified destination port.

Options *destination-port-number* —Number of the destination port for which to display central point session information.

Range: 1 through 65,535

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow cp-session on page 1294**
- **show security flow cp-session destination-prefix on page 1298**

List of Sample Output **show security flow cp-session destination-port summary on page 1297**
show security flow cp-session destination-port terse on page 1297

Output Fields Table 72 on page 1296 lists the output fields for the **show security flow cp-session destination-port** command. Output fields are listed in the approximate order in which they appear.

Table 72: show security flow cp-session destination-port Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

 Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session destination-port summary

```
root> show security flow cp-session destination-port 21 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session destination-port terse

```
root> show security flow cp-session destination-port 21 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

show security flow cp-session destination-prefix

Syntax **show security flow cp-session destination-prefix *destination-IP-prefix* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session-related flow information for the specified destination prefix.

Options *destination-IP-prefix* —Destination IP prefix or address for which to display central point session information.

Range: 1 through 65,535.

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow cp-session on page 1294**
- **show security flow cp-session destination-port on page 1296**

List of Sample Output **show security flow cp-session destination-prefix summary on page 1299**
show security flow cp-session destination-prefix terse on page 1299

Output Fields Table 73 on page 1298 lists the output fields for the **show security flow cp-session destination-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 73: show security flow cp-session destination-prefix Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

 Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session destination-prefix summary

```
root> show security flow cp-session destination-prefix 30/8 summary
Valid sessions: 1
Pending sessions: 1
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2
```

show security flow cp-session destination-prefix terse

```
root> show security flow cp-session destination-prefix 30/8 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

show security flow cp-session family

Syntax **show security flow cp-session family *family* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session-related flow information for the specified family.

Options *family*—Display session by family.

inet—Display IPv4 sessions.

inet6—Display IPv6 and IPv6-NATPT sessions.

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow cp-session on page 1294**

List of Sample Output **show security flow cp-session family summary on page 1301**
show security flow cp-session family terse on page 1301

Output Fields Table 74 on page 1300 lists the output fields for the **show security flow cp-session** family command. Output fields are listed in the approximate order in which they appear.

Table 74: show security flow cp-session family Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

 Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session family summary

```
root> show security flow cp-session family inet summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session family terse

```
root> show security flow cp-session family inet terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

show security flow cp-session protocol

Syntax **show security flow cp-session protocol *protocol-name* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session-related flow information for the specified protocol.

Options *protocol-name* —Protocol to use as a central point session filter. Information about the central point session that uses this protocol is displayed.
Possible protocols are:

ah—IP Security Authentication Header

egp—Exterior gateway protocol

esp—IPsec Encapsulating Security Payload

gre—Generic routing encapsulation

icmp—Internet Control Message Protocol

icmp6—Internet Control Message Protocol

igmp—Internet Group Management Protocol

ipip—IP over IP

ospf—Open Shortest Path First

pim—Protocol Independent Multicast

rsvp—Resource Reservation Protocol

sctp—Stream Control Transmission Protocol

tcp—Transmission Control Protocol

udp—User Datagram Protocol

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow cp-session on page 1294**

List of Sample Output **show security flow cp-session protocol summary on page 1303**
show security flow cp-session protocol terse on page 1303

Output Fields Table 75 on page 1303 lists the output fields for the **show security flow cp-session** protocol command. Output fields are listed in the approximate order in which they appear.

 Copyright © 2011, Juniper Networks, Inc.

Table 75: show security flow cp-session protocol Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

show security flow cp-session protocol summary

```
root> show security flow cp-session protocol tcp summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session protocol terse

```
root> show security flow cp-session protocol tcp terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session source-port

Syntax **show security flow cp-session source-port *source-port-number* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session-related flow information for the specified source-port.

Options *source-port-number*—Number of the source port about which to display central point session information.
Range: 1 through 65,535

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation
- **show security flow cp-session on page 1294**
- **show security flow cp-session source-prefix on page 1306**

List of Sample Output **show security flow cp-session source-port summary on page 1305**
show security flow cp-session source-port terse on page 1305

Output Fields Table 76 on page 1304 lists the output fields for the **show security flow cp-session source-port** command. Output fields are listed in the approximate order in which they appear.

Table 76: show security flow cp-session source-port Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

 Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session source-port summary

```
root> show security flow cp-session source-port 32838 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session source-port terse

```
root> show security flow cp-session source-port 32838 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

show security flow cp-session source-prefix

Syntax **show security flow cp-session source-prefix *source-IP-prefix* [summary | terse]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display central point session related flow information for the specified source-prefix.

Options *source-IP-prefix*—Source IP prefix or address for which to display central point session information.

summary | terse—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow cp-session on page 1294**
- **show security flow cp-session source-port on page 1304**

List of Sample Output **show security flow cp-session source-prefix summary on page 1307**
show security flow cp-session source-prefix terse on page 1307

Output Fields Table 77 on page 1306 lists the output fields for the **show security flow cp-session source-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 77: show security flow cp-session source-prefix Output Fields

Field Name	Field Description
Valid gates	Number of valid central point sessions.
Pending gates	Number of pending central point sessions.
Invalidated gates	Number of invalid central point sessions.
Gates in other states	Number of central point sessions in other states.
Total gates	Number of central point sessions in total.
Session ID	Number that identifies the session. Use this ID to get more information about the session.
SPU	Services Processing Unit.
In	Incoming flow (source and destination IP addresses).
Out	Reverse flow (source and destination IP addresses).

 Copyright © 2011, Juniper Networks, Inc.

show security flow cp-session source-prefix summary

```
root> show security flow cp-session source-prefix 40/8 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session source-prefix terse

```
root> show security flow cp-session source-prefix 40/8 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```

show security flow gate

Syntax

show security flow gate
[<filter>] [brief | summary}

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and display options added in Release 10.2 of Junos OS.

Description

Display information about temporary openings known as pinholes or gates in the security firewall.

Pinholes are used by applications that commonly have both control and data sessions and must create openings in the firewall for the data sessions based on information from the parent sessions.

Options

destination-port—Destination port

destination-prefix—Destination IP prefix or address

protocol—IP protocol number

source-port—Source port

source-prefix—Source IP prefix or address

brief | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **show security flow gate brief node on page 1312**
- **show security flow gate destination-port on page 1318**
- **show security flow gate destination-prefix on page 1321**
- **show security flow gate protocol on page 1326**
- **show security flow gate source-port on page 1329**
- **show security flow gate source-prefix on page 1332**
- **show security flow gate summary node on page 1335**

List of Sample Output

show security flow gate on page 1309
show security flow gate brief on page 1310
show security flow gate summary on page 1311

Output Fields

Table 78 on page 1309 lists the output fields for the **show security flow gate** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2011, Juniper Networks, Inc.

Table 78: show security flow gate Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.
Maximum gates	Number of maximum gates

show security flow gate

```
user@host> show security flow gate
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.252-40.1.1.252/64515-64515
Translated: 0.0.0.0/0->11.0.31.161/25415
Protocol: udp
Application: none/0
Age: 101 seconds
Flags: 0xe001
Zone: untrust
Reference count: 1
Resource: 5-1024-8185
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.252-40.1.1.252/1046-1046
Translated: 40.1.1.250/36039->11.0.31.161/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
Flags: 0xe200
```

```
Zone: untrust
Reference count: 1
Resource: 5-1024-8189
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.5-40.1.1.5/24101-24101
Translated: 0.0.0.0/0->40.1.1.5/24101
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8188
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.5-40.1.1.5/24100-24100
Translated: 0.0.0.0/0->40.1.1.5/24100
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8191
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.250-40.1.1.250/5060-5060
Translated: 0.0.0.0/0->40.1.1.250/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
Flags: 0xe200
Zone: trust
Reference count: 1
Resource: 5-1024-8190
```

show security flow gate brief

```
root> show security flow gate brief
Flow Gates on FPC4 PIC1:

Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/38143-38143
  Translated: 40.0.0.111/0->30.0.0.100/38143
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65532 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate summary

```
root> show security flow gate summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

show security flow gate brief node

Syntax **show security flow gate brief node (*node-id* | all | local | primary)**

Release Information Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified node options in brief mode.

Options **node**—(Optional) For chassis cluster configurations, display gate information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate summary node on page 1335**

List of Sample Output

show security flow gate brief node 0 on page 1313
show security flow gate brief node 1 on page 1314
show security flow gate brief node all on page 1314
show security flow gate brief node local on page 1315
show security flow gate brief node primary on page 1316

Output Fields Table 79 on page 1312 lists the output fields for the **show security flow gate brief node** command. Output fields are listed in the approximate order in which they appear.

Table 79: show security flow gate brief node Output Fields

Field Name	Field Description
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.
Hole	Range of flows permitted by the pinhole.

 Copyright © 2011, Juniper Networks, Inc.

Table 79: show security flow gate brief node Output Fields *(continued)*

Field Name	Field Description
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.

show security flow gate brief node 0

```
root@antbert> show security flow gate brief node 0
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65518 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
```

```
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate brief node 1

```
root@antbert> show security flow gate brief node 1
node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65514 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate brief node all

```
root@antbert> show security flow gate brief node all
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
```


Copyright © 2011, Juniper Networks, Inc.

```
  Age: 65512 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65510 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate brief node local

```
root@antbert> show security flow gate brief node local
node0:
--------------------------------------------------------------------------
```

```
Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65504 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate brief node primary

```
root@antbert> show security flow gate brief node primary
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65500 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate destination-port

Syntax **show security flow gate destination-port *destination-port-number* [brief | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall that for the specified destination port.

NOTE: Destination port filter matches the gate only if the given port falls within the range of ports specified in the gate.

Options *destination-port-number*—Number of the destination port for which to display gate information.

Range: 1 through 65,535

brief | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate destination-prefix on page 1321**

List of Sample Output **show security flow gate destination-port brief on page 1319**
show security flow gate destination-port summary on page 1320

Output Fields Table 80 on page 1318 lists the output fields for the **show security flow gate destination-port** command. Output fields are listed in the approximate order in which they appear.

Table 80: show security flow gate destination-port Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.

 Copyright © 2011, Juniper Networks, Inc.

Table 80: show security flow gate destination-port Output Fields *(continued)*

Field Name	Field Description
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.
Maximum gates	Number of maximum gates.

show security flow gate destination-port brief

```
root> show security flow gate destination-port 33253 brief
Flow Gates on FPC4 PIC1:

Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/33253-33253
  Translated: 40.0.0.111/0->30.0.0.100/33253
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65526 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate destination-port summary

```
root> show security flow gate destination-port 33253 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate destination-prefix

Syntax **show security flow gate destination-prefix *destination-IP-prefix* [brief | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified destination prefix.

NOTE: Destination prefix must match both the starting and ending address in the gate.

Options *destination-IP-prefix*—Destination IP prefix or address for which to display gate information.

brief | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate destination-port on page 1318**

List of Sample Output **show security flow gate destination-prefix brief on page 1322**
show security flow gate destination-prefix summary on page 1322

Output Fields Table 81 on page 1321 lists the output fields for the **show security flow gate destination-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 81: show security flow gate destination-prefix Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.

Copyright © 2011, Juniper Networks, Inc.

Table 81: show security flow gate destination-prefix Output Fields *(continued)*

Field Name	Field Description
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.

show security flow gate destination-prefix brief

```
root> show security flow gate destination-prefix 30.0.0.100 brief
Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/37308-37308
  Translated: 40.0.0.111/0->30.0.0.100/37308
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65456 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24575-86015

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate destination-prefix summary

```
root> show security flow gate destination-prefix 30.0.0.100 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate family

Syntax show security flow gate family (inet | inet6)

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display filtered summary of information about existing gates, types of gates, and the maximum allowed number of gates.

Options inet—Displays IPv4 information.

inet6—Displays IPv6 gate information.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**

Output Fields Table 1 lists the output fields for the **show security flow gate family** command. Output fields are listed in the approximate order in which they appear.

Table 82: show security flow gate family Output Fields

Field Name	Field Description
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Total number of gates.

Sample Output

```
user@host> show security flow gate family inet6
Hole: 2001:13::8-0-0->2001:12::8-33135-33135

  Translated: ::/0->::/0

  Protocol: tcp

  Application: FTP ALG/79

  Age: 24 seconds

  Flags: 0x8080

  Zone: zserver

  Reference count: 1
```


Copyright © 2011, Juniper Networks, Inc.

```
  Resource: 1-2-2


Valid gates: 1

Pending gates: 0

Invalidated gates: 0

Gates in other states: 0

Total gates: 1
```

```
user@host> show security flow gate family inet6 destination-prefix 2001:12::8 or source-prefix
Hole: 2001:13::8-0-0->2001:12::8-33135-33135

  Translated: ::/0->::/0

  Protocol: tcp

  Application: FTP ALG/79

  Age: 26 seconds

  Flags: 0x8080

  Zone: zserver

  Reference count: 1

  Resource: 1-2-2


Valid gates: 1

Pending gates: 0

Invalidated gates: 0

Gates in other states: 0

Total gates: 1
```

show security flow gate protocol

Syntax **show security flow gate protocol *protocol-name* [brief | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified protocol.

Options *protocol-name*—Protocol to use as a gate filter. Information about gates that use this protocol is displayed.

Possible protocols are:

ah—IP Security Authentication Header

egp—Exterior gateway protocol

esp—IPsec Encapsulating Security Payload

gre—Generic routing encapsulation

icmp—Internet Control Message Protocol

icmp6—Internet Control Message Protocol

igmp—Internet Group Management Protocol

ipip—IP over IP

ospf—Open Shortest Path First

pim—Protocol Independent Multicast

rsvp—Resource Reservation Protocol

sctp—Stream Control Transmission Protocol

tcp—Transmission Control Protocol

udp—User Datagram Protocol

brief | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**

List of Sample Output **show security flow gate protocol brief on page 1327**
show security flow gate protocol summary on page 1328

 Copyright © 2011, Juniper Networks, Inc.

Output Fields Table 83 on page 1327 lists the output fields for the **show security flow gate protocol** command. Output fields are listed in the approximate order in which they appear.

Table 83: show security flow gate protocol Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.

show security flow gate protocol brief

```
root> root> show security flow gate protocol tcp brief
Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/37308-37308
  Translated: 40.0.0.111/0->30.0.0.100/37308
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65414 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24575-86015

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
```

```
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate protocol summary

```
root> show security flow gate protocol tcp summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate source-port

Syntax **show security flow gate source-port** ***source-port-number*** **[brief | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified source port.

NOTE: Source port filter matches the gate only if the given port falls within the range of ports specified in the gate.

Options *source-port-number*—Number of the source port for which to display gate information.

Range: 1 through 65,535

brief | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate source-prefix on page 1332**

List of Sample Output **show security flow gate source-port brief on page 1330**
show security flow gate source-port summary on page 1331

Output Fields Table 84 on page 1329 lists the output fields for the **show security flow gate source-port** command. Output fields are listed in the approximate order in which they appear.

Table 84: show security flow gate source-port Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.

Copyright © 2011, Juniper Networks, Inc.

Table 84: show security flow gate source-port Output Fields *(continued)*

Field Name	Field Description
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.

show security flow gate source-port brief

```
root> show security flow gate source-port 5004 brief
Flow Gates on FPC4 PIC1:

Hole: 30.0.0.111-30.0.0.111/5004-5004->40.0.0.100-40.0.0.100/2646-2646
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/0
  Age: 28 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 0-1050869761-1050869762

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate source-port summary

```
root> show security flow gate source-port 5004 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate source-prefix

Syntax **show security flow gate source-prefix** ***source-IP-prefix*** **[brief | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified source prefix.

NOTE: Source prefix must match both the starting and ending address in the gate.

Options *source-IP-prefix* —Source IP prefix or address for which to display gate information.

brief | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate source-port on page 1329**

List of Sample Output **show security flow gate source-prefix brief on page 1333**
show security flow gate source-prefix summary on page 1333

Output Fields Table 85 on page 1332 lists the output fields for the **show security flow gate source-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 85: show security flow gate source-prefix Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.

 Copyright © 2011, Juniper Networks, Inc.

Table 85: show security flow gate source-prefix Output Fields *(continued)*

Field Name	Field Description
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.

show security flow gate source-prefix brief

```
root> show security flow gate source-prefix 30.0.0.100 brief
Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC0:

Hole: 30.0.0.100-30.0.0.100/0-0->40.0.0.111-40.0.0.111/32834-32834
  Translated: 30.0.0.100/0->40.0.0.111/32834
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65442 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate source-prefix summary

```
root> show security flow gate source-prefix 30.0.0.100 summary
Flow Gates on FPC4 PIC1:
```

```
Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate summary node

Syntax **show security flow gate summary node (*node-id* | all | local | primary)**

Release Information Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

Description Display information about temporary openings known as pinholes or gates in the security firewall for the specified node options in summary mode.

Options **node**—(Optional) For chassis cluster configurations, display gate information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- **show security flow gate on page 1308**
- **show security flow gate brief node on page 1312**

List of Sample Output

show security flow gate summary node 0 on page 1336
show security flow gate summary node 1 on page 1337
show security flow gate summary node all on page 1337
show security flow gate summary node local on page 1338
show security flow gate summary node primary on page 1339

Output Fields Table 86 on page 1335 lists the output fields for the **show security flow gate summary node** command. Output fields are listed in the approximate order in which they appear.

Table 86: show security flow gate summary node Output Fields

Field Name	Field Description
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.
Hole	Range of flows permitted by the pinhole.

Table 86: show security flow gate summary node Output Fields *(continued)*

Field Name	Field Description
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.

show security flow gate summary node 0

```
root@antbert> show security flow gate summary node 0
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate summary node 1

```
root@antbert> show security flow gate summary node 1
node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

show security flow gate summary node all

```
root@antbert> show security flow gate summary node all
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

```
node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

show security flow gate summary node local

```
root@antbert> show security flow gate summary node local
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```


Copyright © 2011, Juniper Networks, Inc.

show security flow gate summary node primary

```
root@antbert> show security flow gate summary node primary
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

show security flow ip-action

Syntax **show security flow ip-action**

Release Information Command introduced in Release 10.1 of Junos OS.

Description Display information about currently active security sessions on the device.

Options

- **Src-Addr**—Display information about the source address.
- **Src-Port**—Display information about the source port.
- **Dst-Addr**—Display information about the destination address.
- **Proto/Dst-Port**—Display information about the protocol and destination port.
- **Timeout(sec)**—Display information about timeouts and time remaining.
- **Zone**—Display information about the zone.
- **Action**—Display information about the action type, such as “notify.”

Required Privilege Level view

Related Documentation

- **clear security flow session all on page 1038**

Sample Output

```
user@host> show security flow ip-action
Src-Addr   Src-Port  Dst-Addr   Proto/Dst-Port  Timeout(sec)   Zone     Action
   4.0.0.1    0       0.0.0.0        0/0            10/12        0       notify
```

 Copyright © 2011, Juniper Networks, Inc.

show security flow ip-action family

Syntax show security flow ip-action family (inet | inet6)

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display summary of information about currently active security sessions on the device.

Options inet—Displays IPv4 information.

inet6—Displays IPv6-NATPT information.

Required Privilege Level view

Related Documentation

- show security flow ip-action on page 1340
- clear security flow ip-action family on page 1037

Sample Output `user@host>` show security flow ip-action family inet6

show security flow session

Syntax

show security flow session
[<filter>] [brief | extensive | summary]

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

Description

Display information about all currently active security sessions on the device.

Options

application—Application name

destination-port—Destination port

destination-prefix—Destination IP prefix or address

family—Display session by family.

idp—Display IDP sessions.

interface—Name of incoming or outgoing interface

nat—Display sessions with network address translation.

protocol—IP protocol number

resource-manager—Display sessions with resource manager.

session-identifier—Display sessions with session identifier.

source-port—Source port

source-prefix—Source IP prefix

tunnel—Display tunnel sessions

brief | extensive | summary—Display the specified level of output.

none—Display information about all active sessions.

Required Privilege Level

view

Related Documentation

- **clear security flow session all on page 1038**

List of Sample Output

show security flow session on page 1344
show security flow session brief on page 1344
show security flow session extensive on page 1344
show security flow session summary on page 1345

Output Fields

Table 87 on page 1343 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2011, Juniper Networks, Inc.

Table 87: show security flow session Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

Copyright © 2011, Juniper Networks, Inc.

show security flow session

```
root> show security flow session
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0

root> show security flow session extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0

root> show security flow session extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Status: Normal
Flag: 0x42
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1788
Session State: Valid
Start time: 247, Duration: 12
   In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x40010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 25, Bytes: 1138
```


Copyright © 2011, Juniper Networks, Inc.

```
   Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x50010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 20, Bytes: 1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200
```

Copyright © 2011, Juniper Networks, Inc.

show security flow session application

Syntax

show security flow session application
application-name **[brief | extensive | summary]**

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

Description

Display information about each session of the specified application type.

Options

—

application-name—Type of application about which to display sessions information. Possible values are:

dns—Domain Name System

ftp—File Transfer Protocol

ignore—Ignore application type

mgcp-ca—Media Gateway Control Protocol with Call Agent

mgcp-ua—MGCP with User Agent

pptp—Point-to-Point Tunneling Protocol

q931—ISDN connection control protocol

ras—RAS

realaudio—RealAudio

rsh—UNIX remote shell services

rtsp—Real-Time Streaming Protocol

sccp—Skinny Client Control Protocol

sip—Session Initiation Protocol

sqlnet-v2—Oracle SQLNET

talk—TALK program

tftp—Trivial File Transfer Protocol

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Copyright © 2011, Juniper Networks, Inc.

Related Documentation

- **clear security flow session application on page 1039**

List of Sample Output

show security flow session application telnet on page 1348
show security flow session application telnet brief on page 1348
show security flow session application telnet extensive on page 1348
show security flow session application telnet summary Flow Sessions on FPC4 PIC1: on page 1349

Output Fields

Table 88 on page 1347 lists the output fields for the **show security flow session application** command. Output fields are listed in the approximate order in which they appear.

Table 88: show security flow session application Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.

Copyright © 2011, Juniper Networks, Inc.

Table 88: show security flow session application Output Fields *(continued)*

Field Name	Field Description
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session application telnet

```
root> show security flow session application telnet
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

show security flow session application telnet brief

```
root> show security flow session application telnet brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

show security flow session application telnet extensive

```
root>  show security flow session application telnet extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
```


Copyright © 2011, Juniper Networks, Inc.

```
Session ID: 210067547, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1788
Session State: Valid
Start time: 670184, Duration: 33
   In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1
```

show security flow session application telnet summary Flow Sessions on FPC4 PIC1:

```
root> show security flow session application telnet summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow session brief node

Syntax **show security flow session brief node (*node-id* | all | local | primary)**

Release Information Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

Description Display information about all currently active security sessions on the device for the specified node options in brief mode.

Options **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- **show security flow session on page 1342**

List of Sample Output

show security flow session brief node 0 on page 1351
show security flow session brief node 1 on page 1351
show security flow session brief node all on page 1351
show security flow session brief node local on page 1352
show security flow session brief node primary on page 1352

Output Fields Table 89 on page 1350 lists the output fields for the **show security flow session brief node** command. Output fields are listed in the approximate order in which they appear.

Table 89: show security flow session brief node Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Policy name	Policy that permitted the traffic.
State	Session state.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

 Copyright © 2011, Juniper Networks, Inc.

Table 89: show security flow session brief node Output Fields *(continued)*

Field Name	Field Description
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.

show security flow session brief node 0

```
root@antbert> show security flow session brief node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13978, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session brief node 1

```
root@antbert> show security flow session brief node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Policy name: default-policy/2, State: Active,
Timeout: 1788, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 69, Bytes:
3024
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 62, Bytes:
4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session brief node all

```
root@antbert> show security flow session brief node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:
```

```
Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13972, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Policy name: default-policy/2, State: Active,
Timeout: 1784, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 69, Bytes:
3024
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 62, Bytes:
4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session brief node local

```
root@antbert> show security flow session brief node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13964, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session brief node primary

```
root@antbert> show security flow session brief node primary
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13958, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
```


Copyright © 2011, Juniper Networks, Inc.

```
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session destination-port

Syntax

show security flow session destination-port
destination-port-number **[brief | extensive | summary]**

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

Description

Display information about each session that uses the specified destination port.

Options

destination-port-number —Number of the destination port for which to display sessions information.

Range: 1 through 65,535

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session destination-port on page 1041**

List of Sample Output

show security flow session destination-port 23 on page 1355
show security flow session destination-port 23 brief on page 1356
show security flow session destination-port 23 extensive on page 1356
show security flow session destination-port 23 summary on page 1356

Output Fields

Table 90 on page 1354 lists the output fields for the **show security flow session destination-port** command. Output fields are listed in the approximate order in which they appear.

Table 90: show security flow session destination-port Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.

Copyright © 2011, Juniper Networks, Inc.

Table 90: show security flow session destination-port Output Fields *(continued)*

Field Name	Field Description
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session destination-port 23

```
root> show security flow session destination-port 23
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Policy name: default-policy/2, Timeout: 1798, Valid
  In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

```
Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-port 23 brief

```
root> show security flow session destination-port 23 brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Policy name: default-policy/2, Timeout: 1798, Valid
  In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-port 23 extensive

```
root> show security flow session destination-port 23 extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1794
Session State: Valid
Start time: 670359, Duration: 26
   In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-port 23 summary

```
root> show security flow session destination-port 23 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session destination-prefix

Syntax

show security flow session destination-prefix
destination-IP-prefix **[brief | extensive | summary]**

Release Information

Command introduced in Release 8.5 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.
Filter and view options added in Release 10.2 of Junos OS.

Description

Display information about each session that matches the specified IP destination prefix.

Options

destination-IP-prefix—Destination IP prefix or address for which to display session information.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session destination-prefix on page 1042**

List of Sample Output

show security flow session destination-prefix 30/8 on page 1359
show security flow session destination-prefix 30/8 brief on page 1360
show security flow session destination-prefix 30/8 extensive on page 1360
show security flow session destination-prefix 30/8 summary on page 1360
show security flow session destination-prefix 10::10 on page 1361

Output Fields

Table 91 on page 1358 lists the output fields for the **show security flow session destination-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 91: show security flow session destination-prefix Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

Copyright © 2011, Juniper Networks, Inc.

Table 91: show security flow session destination-prefix Output Fields *(continued)*

Field Name	Field Description
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session destination-prefix 30/8

```
root> show security flow session destination-prefix 30/8
Flow Sessions on FPC4 PIC1:

Session ID: 170068346, Policy name: default-policy/2, Timeout: 1792, Valid
  In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 11, Bytes:
662
  Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes:
708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0
```

```
Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-prefix 30/8 brief

```
root> show security flow session destination-prefix 30/8 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068346, Policy name: default-policy/2, Timeout: 1792, Valid
  In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 11, Bytes:
662
  Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes:
708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-prefix 30/8 extensive

```
root> show security flow session destination-prefix 30/8 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068346, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1780
Session State: Valid
Start time: 670272, Duration: 40
   In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 662
   Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-prefix 30/8 summary

```
root> show security flow session destination-prefix 30/8 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2011, Juniper Networks, Inc.

```
Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session destination-prefix 10::10

```
user@host> show security flow session destination-prefix 10::10
Session ID: 50000004, Policy name: self-traffic-policy/1, Timeout: 2
In: 10::11/42756 --> 10::10/0;icmp, If: .local..0
Out: 10::10/0 --> 10::11/42756;icmp, If: ge-0/3/0.0

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow session extensive node

Syntax **show security flow session extensive node (*node-id* | all | local | primary)**

Release Information Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

Description Display information about all currently active security sessions on the device for the specified node options in extensive mode.

Options **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- **show security flow session on page 1342**

List of Sample Output

show security flow session extensive node 0 on page 1363
show security flow session extensive node 1 on page 1364
show security flow session extensive node all on page 1364
show security flow session extensive node local on page 1365
show security flow session extensive node primary on page 1366

Output Fields Table 92 on page 1362 lists the output fields for the **show security flow session extensive node** command. Output fields are listed in the approximate order in which they appear.

Table 92: show security flow session extensive node Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Status	Session status.
State	Session state.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Policy that permitted the traffic.
Source NAT pool	The name of the source pool where NAT is used.

 Copyright © 2011, Juniper Networks, Inc.

Table 92: show security flow session extensive node Output Fields *(continued)*

Field Name	Field Description
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Start time	Time when the session was created, offset from the system start time.
Duration	Length of time for which the session is active.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, flag, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, flag, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.

show security flow session extensive node 0

```
root@antbert> show security flow session extensive node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13946
Session State: Valid
Start time: 2021, Duration: 469
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session extensive node 1

```
root@antbert> show security flow session extensive node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Status: Normal, State: Active
Flag: 0x8000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1756
Session State: Valid
Start time: 2023, Duration: 473
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x84863c2, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 69, Bytes: 3024
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x84843c2, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 62, Bytes: 4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session extensive node all

```
root@antbert> show security flow session extensive node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13936
Session State: Valid
Start time: 2021, Duration: 478
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Status: Normal, State: Active
Flag: 0x8000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1750
Session State: Valid
Start time: 2023, Duration: 479
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x84863c2, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 69, Bytes: 3024
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x84843c2, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 62, Bytes: 4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session extensive node local

```
root@antbert> show security flow session extensive node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13930
Session State: Valid
```

```
Start time: 2021, Duration: 484
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

show security flow session extensive node primary

```
root@antbert> show security flow session extensive node primary
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13924
Session State: Valid
Start time: 2021, Duration: 490
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session family

Syntax

show security flow session family (inet | inet6)
[brief | extensive | summary]

Release Information

Command introduced in Release 10.2 of Junos OS.

Description

Display filtered summary of information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.

Options

inet—Display details summary of IPv4 sessions.

inet6—Display details summary of IPv6 sessions.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session family on page 1044**

List of Sample Output

show security flow session family inet on page 1368
show security flow session family inet brief on page 1369
show security flow session family inet extensive on page 1369
show security flow session family inet summary on page 1370

Output Fields

Table 93 on page 1367 lists the output fields for the **show security flow session family** command. Output fields are listed in the approximate order in which they appear.

Table 93: show security flow session family Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.

Copyright © 2011, Juniper Networks, Inc.

Table 93: show security flow session family Output Fields *(continued)*

Field Name	Field Description
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session family inet

```
root> show security flow session family inet
Flow Sessions on FPC4 PIC1:

Session ID: 170067516, Policy name: self-traffic-policy/1, Timeout: 4, Valid
  In: 40.0.0.100/23 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/23;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066737, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/21 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/21;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066726, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/22 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
```


Copyright © 2011, Juniper Networks, Inc.

```
  Out: 40.0.0.1/26637 --> 40.0.0.100/22;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1
```

show security flow session family inet brief

```
root> show security flow session family inet brief
Flow Sessions on FPC4 PIC1:

Session ID: 170067516, Policy name: self-traffic-policy/1, Timeout: 4, Valid
  In: 40.0.0.100/23 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/23;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066737, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/21 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/21;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066726, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/22 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/22;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1
```

show security flow session family inet extensive

```
root> show security flow session family inet extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170067527, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 667332, Duration: 1
   In: 40.0.0.100/56 --> 40.0.0.1/26637;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/56;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066749, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 667329, Duration: 1
   In: 40.0.0.100/57 --> 40.0.0.1/26637;icmp,
```

```
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/57;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066737, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 667326, Duration: 3
   In: 40.0.0.100/55 --> 40.0.0.1/26637;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/55;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

show security flow session family inet summary

```
root> show security flow session family inet summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 1
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Invalidated sessions: 1
Sessions in other states: 0
Total sessions: 2
```

show security flow session idp summary

Syntax **show security flow session idp summary**

Release Information Command introduced in Release 10.2 of Junos OS

Description Display summary output.

Options application—Application name

destination-port—Destination port

destination-prefix—Destination IP prefix or address

family—Display session by family.

interface—Name of incoming or outgoing interface

protocol—IP protocol number

source-port—Source port

source-prefix—Source IP prefix

Required Privilege Level view

Related Documentation

- **show security flow session on page 1342**

List of Sample Output **show security flow session idp summary on page 1372**

Output Fields Table 94 on page 1372 lists the output fields for the **show security flow session idp summary** command. Output fields are listed in the approximate order in which they appear.

Table 94: show security flow session idp summary Output Fields

Field Name	Field Description
Valid session	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalid sessions.
Sessions in other states	Number of sessions in other states.
Total sessions	Total number of sessions.

show security flow session idp summary

```
root@ show security flow session idp summary
Flow Sessions on FPC4 PIC0:
```


Copyright © 2011, Juniper Networks, Inc.

```
Valid sessions: 3
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 3

Flow Sessions on FPC5 PIC0:

Valid sessions: 4
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 4
```

show security flow session interface

Syntax

show security flow session interface
interface-name **[brief | extensive | summary]**

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

Description

Display information about each session that uses the specified interface. The interface name can be a session's incoming or outgoing interface.

Options

interface-name—Name of the interface on the device for which to display sessions information.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session interface on page 1045**

List of Sample Output

show security flow session interface ge-0/0/2.0 on page 1375
show security flow session interface ge-0/0/2.0 brief on page 1376
show security flow session interface ge-0/0/2.0 extensive on page 1376
show security flow session interface ge-0/0/2.0 summary on page 1377

Output Fields

Table 95 on page 1374 lists the output fields for the **show security flow session interface** command. Output fields are listed in the approximate order in which they appear.

Table 95: show security flow session interface Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.

Copyright © 2011, Juniper Networks, Inc.

Table 95: show security flow session interface Output Fields *(continued)*

Field Name	Field Description
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session interface ge-0/0/2.0

```
root> show security flow session interface ge-0/0/2.0
Flow Sessions on FPC4 PIC1:

Session ID: 170068353, Policy name: default-policy/2, Timeout: 4, Valid
  In: 40.0.0.100/18 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/18;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067569, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/16 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/16;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

Copyright © 2011, Juniper Networks, Inc.

```
Flow Sessions on FPC5 PIC1:

Session ID: 210067554, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/17 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/17;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

show security flow session interface ge-0/0/2.0 brief

```
root> show security flow session interface ge-0/0/2.0 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068353, Policy name: default-policy/2, Timeout: 4, Valid
  In: 40.0.0.100/18 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/18;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067569, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/16 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/16;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067554, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/17 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/17;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

show security flow session interface ge-0/0/2.0 extensive

```
root> show security flow session interface ge-0/0/2.0 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068354, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670502, Duration: 2
   In: 40.0.0.100/21 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/21;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
```


Copyright © 2011, Juniper Networks, Inc.

```
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067571, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670500, Duration: 1
   In: 40.0.0.100/22 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/22;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067556, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670499, Duration: 1
   In: 40.0.0.100/23 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/23;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

show security flow session interface ge-0/0/2.0 summary

```
root> show security flow session interface ge-0/0/2.0 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

```
Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session nat

Syntax **show security flow session nat [brief | extensive | summary]**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display sessions with network address translation.

Options brief | extensive | summary—Display the specified level of output.

Required Privilege Level view

Related Documentation
- **show security flow session on page 1342**

List of Sample Output
show security flow session nat brief on page 1380
show security flow session nat extensive on page 1380
show security flow session nat summary on page 1381

Output Fields Table 96 on page 1379 lists the output fields for the **show security flow session nat** command. Output fields are listed in the approximate order in which they appear.

Table 96: show security flow session nat Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
Resource information	Information about the session particular to the resource manager, including the name of the ALG, the group ID. and the resource ID.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.

Copyright © 2011, Juniper Networks, Inc.

Table 96: show security flow session nat Output Fields *(continued)*

Field Name	Field Description
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.

show security flow session nat brief

```
root> show security flow session nat brief
Flow Sessions on FPC4 PIC1:

Session ID: 170000019, Policy name: idp/4, Timeout: 1790, Valid
  In: 40.0.0.111/32817 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 13, Bytes:
610
  Out: 30.0.0.100/21 --> 30.0.0.1/64508;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes: 640
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session nat extensive

```
root> show security flow session nat extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170000019, Status: Normal
Flag: 0x2
Policy name: idp/4
Source NAT pool: interface, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1784
Session State: Valid
Start time: 1780, Duration: 16
   In: 40.0.0.111/32817 --> 30.0.0.100/21;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x40010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
```


Copyright © 2011, Juniper Networks, Inc.

```
    Pkts: 13, Bytes: 610
   Out: 30.0.0.100/21 --> 30.0.0.1/64508;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x50010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 640
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session nat summary

```
root> show security flow session nat summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session protocol

Syntax

show security flow session protocol (*protocol-name* | *protocol-number*)
[brief | extensive | summary]

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

Description

Display information about each session that uses the specified protocol.

Options

protocol-name —(Optional) Protocol to use as a sessions filter. Information about sessions that use this protocol is displayed. Possible protocols are:

- **ah**—IP Security Authentication Header
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload
- **gre**—Generic routing encapsulation
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP over IP
- **ospf**—Open Shortest Path First
- **pim**—Protocol Independent Multicast
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

protocol-number —(Optional) Numeric protocol value. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers* (*for the Internet Protocol Suite*).

Range: 0 through 255

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session protocol on page 1046**

List of Sample Output

show security flow session protocol icmp on page 1384
show security flow session protocol icmp brief on page 1384
show security flow session protocol icmp extensive on page 1385
show security flow session protocol icmp summary on page 1386

Copyright © 2011, Juniper Networks, Inc.

Output Fields Table 97 on page 1383 lists the output fields for the **show security flow session protocol** command. Output fields are listed in the approximate order in which they appear.

Table 97: show security flow session protocol Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.

Copyright © 2011, Juniper Networks, Inc.

Table 97: show security flow session protocol Output Fields *(continued)*

Field Name	Field Description
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session protocol icmp

```
root> show security flow session protocol icmp
Flow Sessions on FPC4 PIC1:

Session ID: 170068388, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/121 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/121;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067603, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/119 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/119;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067588, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/120 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/120;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

show security flow session protocol icmp brief

```
root> show security flow session protocol icmp brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068388, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/121 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/121;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067603, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/119 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/119;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
```


Copyright © 2011, Juniper Networks, Inc.

```
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067588, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/120 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/120;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

show security flow session protocol icmp extensive

```
root> show security flow session protocol icmp extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068389, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670605, Duration: 2
   In: 40.0.0.100/124 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/124;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067605, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 670603, Duration: 1
   In: 40.0.0.100/125 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/125;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

```
Flow Sessions on FPC5 PIC1:

Session ID: 210067590, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 670602, Duration: 1
   In: 40.0.0.100/126 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/126;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

show security flow session protocol icmp summary

```
root> show security flow session protocol icmp summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session resource-manager

Syntax

show security flow session resource-manager
[brief | extensive | summary]

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

Description

Display information about sessions created by the resource manager.

Options

none—Display all resource manager sessions.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session resource-manager on page 1048**

List of Sample Output

show security flow session resource-manager on page 1388
show security flow session resource-manager brief on page 1389
show security flow session resource-manager extensive on page 1389
show security flow session resource-manager summary on page 1390

Output Fields

Table 98 on page 1387 lists the output fields for the **show security flow session resource-manager** command. Output fields are listed in the approximate order in which they appear.

Table 98: show security flow session resource-manager Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
Resource information	Information about the session particular to the resource manager, including the name of the ALG, the group ID. and the resource ID.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.

Copyright © 2011, Juniper Networks, Inc.

Table 98: show security flow session resource-manager Output Fields *(continued)*

Field Name	Field Description
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.

show security flow session resource-manager

```
root> show security flow session resource-manager
Flow Sessions on FPC4 PIC1:

Session ID: 170068496, Policy name: default-policy/2, Timeout: 1798, Valid
Resource information : FTP ALG, 24576, 0
  In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 82, Bytes:
3964
  Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp, If: ge-0/0/1.0, Pkts: 72, Bytes:
4998

Session ID: 170068501, Policy name: default-policy/2, Timeout: 150, Valid
Resource information : FTP ALG, 24576, 86016
  In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp, If: ge-0/0/1.0, Pkts: 53637, Bytes:
 79808988
  Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp, If: ge-0/0/2.0, Pkts: 20856, Bytes:
 1084520
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session resource-manager brief

```
root> show security flow session resource-manager brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068496, Policy name: default-policy/2, Timeout: 1798, Valid
Resource information : FTP ALG, 24576, 0
  In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 82, Bytes:
3964
  Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp, If: ge-0/0/1.0, Pkts: 72, Bytes:
4998

Session ID: 170068501, Policy name: default-policy/2, Timeout: 150, Valid
Resource information : FTP ALG, 24576, 86016
  In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp, If: ge-0/0/1.0, Pkts: 53637, Bytes:
 79808988
  Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp, If: ge-0/0/2.0, Pkts: 20856, Bytes:
 1084520
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session resource-manager extensive

```
root> show security flow session resource-manager extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068496, Status: Normal
Flag: 0x42
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 672899, Duration: 110
Client: FTP ALG, Group: 24576, Resource: 0
   In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x90010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 84, Bytes: 4044
   Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 74, Bytes: 5116

Session ID: 170068501, Status: Normal
Flag: 0x80001040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 2, Current timeout: 2
Session State: Valid
Start time: 673004, Duration: 5
Client: FTP ALG, Group: 24576, Resource: 86016
   In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp,
    Interface: ge-0/0/1.0,
```

```
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 177002, Bytes: 263785189
   Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x20
    Route: 0x90010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 66402, Bytes: 3452912
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session resource-manager summary

```
root> show security flow session resource-manager summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session session-identifier

Syntax
show security flow session session-identifier
session-identifier

Release Information
Command introduced in Release 8.5 of Junos OS;

Description
Display detailed information for the session with this identifier.

Options
session-identifier —Identifier of the session about which to display information.

Required Privilege Level
view

Related Documentation
- **clear security flow session session-identifier on page 1049**

List of Sample Output
show security flow session session-identifier 36 on page 1392
show security flow session session-identifier 2218 on page 1392
show security flow session session-identifier 33 on page 1393

Output Fields
Table 99 on page 1391 lists the output fields for the **show security flow session session-identifier** command. Output fields are listed in the approximate order in which they appear.

Table 99: show security flow session session-identifier Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Virtual system	Virtual system to which the session belongs.
Policy name	Name and ID of the policy that the first packet of the session matched.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Start time	Time when the session was created, offset from the system start time.
Duration	Length of time for which the session is active.

Copyright © 2011, Juniper Networks, Inc.

Table 99: show security flow session session-identifier Output Fields *(continued)*

Field Name	Field Description
In	For the input flow: • Source and destination addresses and protocol tuple for the input flow. • **Interface**: Input flow interface. • **Session token**: Internal token derived from the virtual routing instance. • **Flag**: Internal debugging flags. • **Route**: Internal next hop of the route to be used by the flow. • **Gateway**: Next-hop gateway of the flow. • **Tunnel**: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero). • **Port Sequence, FIN sequence, FIN state, Cookie**: Internal TCP state tracking information.
Out	For the reverse flow: • Source and destination addresses, and protocol tuple for the reverse flow. • **Interface**: Reverse flow interface. • **Session token**: Internal token derived from the virtual routing instance. • **Flag**: Internal debugging flags. • **Route**: Internal next hop of the route to be used by the flow. • **Gateway**: Next-hop gateway of the flow. • **Tunnel**: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero). • **Port Sequence, FIN sequence, FIN state, Cookie**: Internal TCP state tracking information.

show security flow session session-identifier 36

```
user@host> show security flow session session-identifier 36
Session ID: 36, Status: Normal, Flag: 0x8094540
Virtual system: Root VSYS(I), Policy name: foo/4
Maximum timeout: 1800, Current timeout: 1646
Start time: 61995, Duration: 158
   In: 10.10.10.1/4923 --> 3.3.3.2/23;tcp,
    Interface: t1-1/0/0.0,
    Session token: 0x12, Flag: 0x8094530
    Route: 0x70010, Gateway: 10.10.10.0, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 3.3.3.2/23 --> 10.10.10.1/4923;tcp,
    Interface: .local..0,
    Session token: 0x4, Flag: 0x8094530
    Route: 0xfffb0006, Gateway: 3.3.3.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```

show security flow session session-identifier 2218

```
user@host> show security flow session session-identifier 2218
Session ID: 2218, Status: Normal, Flag: 0x8094660
Virtual system: Root VSYS(I), Policy name: foo/4
Maximum timeout: 60, Current timeout: 60
Start time: 0, Duration: 0
Client: MGCP ALG, Group: 2047, Resource: 8188
   In: 12.0.102.26/28072 --> 11.0.101.236/23252;udp,
    Interface: ge-0/0/2.0,
    Session token: 0xa, Flag: 0x8094740
    Route: 0xb0010, Gateway: 12.0.102.26, Tunnel: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 11.0.101.236/23252 --> 12.0.102.26/28072;udp,
    Interface: ge-0/0/1.0,
    Session token: 0x8, Flag: 0x8094740
Route: 0xa0010, Gateway: 11.0.101.236, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```

show security flow session session-identifier 33

```
user@host> show security flow session session-identifier 33
Session ID: 33, Status: Normal, Flag: 0x80a15f0
Virtual system: Root VSYS(I), Policy name: default-policy/2
Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1492
Start time: 31128, Duration: 121
   In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp,
    Interface: t1-1/0/0.0,
Session token: 0x6, Flag: 0x80a15e0
    Route: 0x60010, Gateway: 10.10.10.0, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x6, Flag: 0x80a15e0
    Route: 0x90010, Gateway: 192.168.0.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```

show security flow session source-port

Syntax

show security flow session source-port
source-port-number
[brief | extensive | summary]

Release Information

Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

Description

Display information about each session that uses the specified source port.

Options

source-port-number —Number of the source port about which to display sessions information.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session source-port on page 1050**

List of Sample Output

show security flow session source-port 32785 on page 1395
show security flow session source-port 32785 brief on page 1395
show security flow session source-port 32785 extensive on page 1396
show security flow session source-port 32785 summary on page 1396

Output Fields

Table 100 on page 1394 lists the output fields for the **show security flow session source-port** command. Output fields are listed in the approximate order in which they appear.

Table 100: show security flow session source-port Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
Resource information	Information about the session particular to the resource manager, including the name of the ALG, the group ID, and the resource ID.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

Copyright © 2011, Juniper Networks, Inc.

Table 100: show security flow session source-port Output Fields *(continued)*

Field Name	Field Description
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.

show security flow session source-port 32785

```
root> show security flow session source-port 32785
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1758, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-port 32785 brief

```
root> show security flow session source-port 32785 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1758, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
```

```
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-port 32785 extensive

```
root> show security flow session source-port 32785 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1754
Session State: Valid
Start time: 670711, Duration: 67
   In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-port 32785 summary

```
root> show security flow session source-port 32785 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:
```


Copyright © 2011, Juniper Networks, Inc.

```
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session source-prefix

Syntax

show security flow session source-prefix
source-prefix-number
[brief | extensive | summary]

Release Information

Command introduced in Release 8.5 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.
Filter and view options introduced in Release 10.2 of Junos OS.

Description

Display information about each session that uses the specified source prefix.

Options

source-prefix-number—Source IP prefix or address for which to display sessions information.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **clear security flow session source-prefix on page 1051**

List of Sample Output

show security flow session source-prefix 40/8 on page 1399
show security flow session source-prefix 40/8 brief on page 1399
show security flow session source-prefix 40/8 extensive on page 1400
show security flow session source-prefix 40/8 summary on page 1400

Output Fields

Table 101 on page 1398 lists the output fields for the **show security flow session source-prefix** command. Output fields are listed in the approximate order in which they appear.

Table 101: show security flow session source-prefix Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

Copyright © 2011, Juniper Networks, Inc.

Table 101: show security flow session source-prefix Output Fields *(continued)*

Field Name	Field Description
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.

show security flow session source-prefix 40/8

```
root> show security flow session source-prefix 40/8
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1784, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 3, Bytes: 194

  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 2, Bytes:
112
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-prefix 40/8 brief

```
root> show security flow session source-prefix 40/8 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1784, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 3, Bytes: 194
```

```
  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 2, Bytes:
112
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-prefix 40/8 extensive

```
root> show security flow session source-prefix 40/8 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 670711, Duration: 21
   In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session source-prefix 40/8 summary

```
root> show security flow session source-prefix 40/8 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:
```


Copyright © 2011, Juniper Networks, Inc.

```
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session summary family

Syntax show security flow session summary family (inet | inet6)

Release Information Command introduced in Release 10.2 of Junos OS.
Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.
Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.

Description Display filtered summary of information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.

Options **inet**—Display details summary of IPv4 sessions.

inet6—Display details summary of IPv6 sessions.

Required Privilege Level view

Related Documentation
- **clear security flow session all on page 1038**

List of Sample Output **show security flow session summary family inet on page 1402**
show security flow session summary family inet6 on page 1403

Output Fields Table 102 on page 1402 lists the output fields for the **show security flow session summary family** command. Output fields are listed in the approximate order in which they appear.

Table 102: show security flow session summary Output Fields

Field Name	Field Description
Valid sessions	Count of valid sessions.
Pending sessions	Count of pending sessions.
Invalidated sessions	Count of sessions the security device has determined to be invalid.
Sessions in other states	Count of sessions not in valid, pending, or invalidated state.
Total sessions	Total of the above counts.

show security flow session summary family inet

```
user@host> show security flow session summary family inet
Session summary for family inet:
Valid sessions: 20
Pending sessions: 0
Invalidated sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Sessions in other states: 0
Total sessions: 20
```

show security flow session summary family inet6

```
user@host> show security flow session summary family inet6
Session summary for family inet6:
Valid sessions: 20
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 20
```

show security flow session summary node

Syntax **show security flow session summary node (*node-id* | all | local | primary)**

Release Information Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.
Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.
Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.

Description Display information about all currently active security sessions on the device for the specified node options in summary mode.

Options **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation
- **show security flow session on page 1342**

List of Sample Output
show security flow session summary node 0 on page 1405
show security flow session summary node 1 on page 1405
show security flow session summary node all on page 1406
show security flow session summary node local on page 1407
show security flow session summary node primary on page 1408

Output Fields Table 103 on page 1404 lists the output fields for the **show security flow session summary node** command. Output fields are listed in the approximate order in which they appear.

Table 103: show security flow session summary node Output Fields

Field Name	Field Description
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.

Copyright © 2011, Juniper Networks, Inc.

Table 103: show security flow session summary node Output Fields *(continued)*

Field Name	Field Description
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

show security flow session summary node 0

```
root@antbert> show security flow session summary node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

show security flow session summary node 1

```
root@antbert> show security flow session summary node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
```

```
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

show security flow session summary node all

```
root@antbert> show security flow session summary node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
```

 Copyright © 2011, Juniper Networks, Inc.

```
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

show security flow session summary node local

```
root@antbert> show security flow session summary node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
```

```
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

show security flow session summary node primary

```
root@antbert> show security flow session summary node primary
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```


Copyright © 2011, Juniper Networks, Inc.

show security flow session tunnel

Syntax
show security flow session tunnel
[brief | extensive | summary]

Release Information
Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

Description
Display information about all tunnel sessions.

Options
none—Display all tunnel sessions.

brief | extensive | summary—Display the specified level of output.

Required Privilege Level
view

List of Sample Output
show security flow session tunnel on page 1410
show security flow session tunnel brief on page 1410
show security flow session tunnel extensive on page 1411
show security flow session tunnel summar on page 1412

Output Fields
Table 104 on page 1409 lists the output fields for the **show security flow session tunnel** command. Output fields are listed in the approximate order in which they appear.

Table 104: show security flow session tunnel Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic. NA (Not Applicable) for a tunnel session.
Timeout	Idle timeout after which the session expires. NA (Not Applicable) for a tunnel session.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.

Copyright © 2011, Juniper Networks, Inc.

Table 104: show security flow session tunnel Output Fields *(continued)*

Field Name	Field Description
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.

show security flow session tunnel

```
root> show security flow session tunnel
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/513;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 170000328, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 200000326, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session tunnel brief

```
root> show security flow session tunnel brief
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/513;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 170000328, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
```


Copyright © 2011, Juniper Networks, Inc.

```
Session ID: 200000326, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session tunnel extensive

```
root> show security flow session tunnel extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8073, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/513;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x4000621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Session ID: 170000328, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8073, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8072, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x4000621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Session ID: 200000326, Status: Normal
Flag: 0x10000
```

```
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8072, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session tunnel summar

```
root> show security flow session tunnel summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security flow statistics

Syntax **show security flow statistics**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display flow-related system statistics.

Required Privilege Level view

List of Sample Output **show security flow statistics on page 1413**

Output Fields Table 105 on page 1413 lists the output fields for the **show security flow statistics** command. Output fields are listed in the approximate order in which they appear.

Table 105: show security flow statistics Output Fields

Field Name	Field Description
Current sessions	Number of current sessions.
Packets forwarded	Number of packets forwarded.
Packets dropped	Number of Packets dropped.
Fragment packets	Number of fragment packets.

show security flow statistics

```
root> show security flow statistics
Flow Statistics of FPC4 PIC1:
    Current sessions: 63
    Packets forwarded: 3001
    Packets dropped: 1281
    Fragment packets: 0

  Flow Statistics of FPC5 PIC0:
    Current sessions: 22
    Packets forwarded: 859
    Packets dropped: 0
    Fragment packets: 0

  Flow Statistics of FPC5 PIC1:
    Current sessions: 22
    Packets forwarded: 858
    Packets dropped: 0
    Fragment packets: 0

  Flow Statistics Summary:
    System total valid sessions: 107
    Packets forwarded: 4718
    Packets dropped: 1281
    Fragment packets: 0
```

Copyright © 2011, Juniper Networks, Inc.

show security flow status

Syntax **show security flow status**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the flow processing modes and logging status.

Required Privilege Level view

List of Sample Output **show security flow status on page 1414**

Output Fields Table 106 on page 1414 lists the output fields for the **show security flow status** command. Output fields are listed in the approximate order in which they appear.

Table 106: show security flow status Output Fields

Field Name	Field Description
Flow forwarding mode	Flow processing mode. • Inet forwarding mode • Inet6 forwarding mode • MPLS forwarding mode • ISO forwarding mode
Flow trace status	Flow logging status. • Flow tracing status • Flow tracing options

show security flow status

```
root> show security flow status
  Flow forwarding mode:
    Inet forwarding mode: flow based
    Inet6 forwarding mode: flow based
    MPLS forwarding mode: drop
    ISO forwarding mode: drop
  Flow trace status
    Flow tracing status: on
    Flow tracing options: all
```


Copyright © 2011, Juniper Networks, Inc.

show security gprs sctp counters

Syntax **show security gprs sctp counters**

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the statistics of the received and dropped Stream Control Transmission Protocol (SCTP) packets.

Options none—Display the statistics of all received and dropped SCTP packets.

Required Privilege Level view

Related Documentation
- **clear security gprs sctp counters on page 1052**

List of Sample Output **show security gprs sctp counters on page 1415**

Output Fields Table 107 on page 1415 lists the output fields for the **show security gprs sctp counters** command. Output fields are listed in the approximate order in which they appear.

Table 107: show security gprs sctp counters

Field Name	Field Description
Name	Name of the SCTP payload protocol identifier.
Received Counter	Number of SCTP packet counters received.
Drop Counter	Number of SCTP packet counters dropped due to error.

show security gprs sctp counters

```
user@host> show security gprs sctp counters
Received/Dropped SCTP packet counters:
Name            Recevied Counter    Drop Counter
reserved        0                   0
iua             0                   0
m2ua            0                   0
m3ua            0                   0
sua             0                   0
m2pa            0                   0
v5ua            0                   0
h248            0                   0
bicc            0                   0
tali            0                   0
dua             0                   0
asap            0                   0
enrp            0                   0
h323            0                   0
qipc            0                   0
simco           0                   0
```

show security group-vpn member ike security-associations

Syntax show security group-vpn member ike security-associations [brief | detail] [index *sa-index*] [*peer-ipaddress*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display IKE security associations (SAs) for a group member.

Options none—Display summary information about all IKE SAs for the group member.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed output.

index *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

peer-ipaddress—(Optional) Display information about the SA with the specified peer.

Required Privilege Level view

Related Documentation

- **clear security group-vpn member ike security-associations on page 1053**

List of Sample Output **show security group-vpn member ike security-associations on page 1418**
show security group-vpn member ike security-associations detail on page 1418

Output Fields Table 108 on page 1416 lists the output fields for the **show security group-vpn member ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 108: show security group-vpn member ike security-associations Output Fields

Field Name	Field Description
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Remote Address	IP address of the destination peer with which the local peer communicates.
State	State of the IKE security associations: • **DOWN**—SA has not been negotiated with the peer. • **UP**—SA has been negotiated with the peer.
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.

Copyright © 2011, Juniper Networks, Inc.

Table 108: show security group-vpn member ike security-associations Output Fields *(continued)*

Field Name	Field Description
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.
Mode	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are • **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
IKE Peer	IP address of the destination peer with which the local peer communicates.
Exchange type	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are • **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
Authentication method	Method the server uses to authenticate the source of IKE messages: • **pre-shared-keys**—Preshared key for encryption and decryption that both participants must have before beginning tunnel negotiations. **rsa-signatures** —Digital signature, a certificate that confirms the identity of the certificate holder.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Copyright © 2011, Juniper Networks, Inc.

Table 108: show security group-vpn member ike security-associations Output Fields *(continued)*

Field Name	Field Description

Algorithms	Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:
	• **Authentication**—Type of authentication algorithm used.
	  • **sha1**—Secure Hash Algorithm 1(sha1) authentication.
	  • **md5**—MD5 authentication.
	• **Encryption**—Type of encryption algorithm used.
	  • **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.
	  • **aes-192-cbc**— AES192-bit encryption
	  • **aes-128-cbc**—AES 128-bit encryption.
	  • **3des-cbc**—3 Data Encryption Standard (DES) encryption.
	  • **des-cbc**—DES encryption.

Traffic statistics	• **Input bytes—**Number of bytes received. • **Output bytes—**Number of bytes transmitted. • **Input packets—**Number of packets received. • **Output packets—**Number of packets transmitted.
IPSec security associations	• ***number* created:** The number of SAs created. • ***number* deleted**: The number of SAs deleted.

Phase 2 negotiations in progress	Number of Phase 2 IKE negotiations in progress and status information:
	• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.
	• **Message ID**—Unique identifier for a Phase 2 negotiation.
	• **Local identity**—Identity of the local Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)
	• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)
	• **Flags**—Notification to the key management process of the status of the IKE negotiation:
	  • **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.

show security group-vpn member ike security-associations

```
user@host> show security group-vpn member ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
1       10.1.1.11       UP     a9b023fbdc7a6571  a67cefbc3397c3c2  Main
```

show security group-vpn member ike

```
user@host> show security group-vpn member ike security-associations detail
IKE peer 10.1.1.11, Index 411,
  Role: Initiator, State: UP
```


Copyright © 2011, Juniper Networks, Inc.

security-associations detail

```
Initiator cookie: 941108c6c186324a, Responder cookie: 0000000000000000
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.1.13:848, Remote: 10.1.1.11:848
Lifetime: Expires in 3536 seconds
Algorithms:
 Authentication        : unknown
 Encryption            : unknown
 Pseudo random function: unknown
Traffic statistics:
 Input  bytes  :                    0
 Output bytes  :                  560
 Input  packets:                    0
 Output packets:                    4
IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 0
```

show security group-vpn member ipsec security-associations

Syntax show security group-vpn member ipsec security-associations [brief | detail] [index *sa-index*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display group VPN security associations (SAs) for a group member.

Options none—Display information about all group VPN SAs for the group member.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed output.

index *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

Required Privilege Level view

Related Documentation

- **clear security group-vpn member ipsec security-associations on page 1054**

List of Sample Output **show security group-vpn member ipsec security-associations on page 1422**
show security group-vpn member ipsec security-associations detail on page 1422

Output Fields Table 109 on page 1420 lists the output fields for the **show security group-vpn member ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 109: show security group-vpn member ipsec security-associations

Field Name	Field Description
Total active tunnels	Total number of active IPsec tunnels.
ID	Index number of the SA. You can use this number to get additional information about the SA.
Server	IP address of the group server (remote gateway).
Port	If Network Address Translation-Traversal (NAT-T) is used, this value is 4500. Otherwise it is the standard IKE port, 500.
Algorithm	Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes • An authentication algorithm used to authenticate exchanges between the peers. Options are **sha1** or **md5.** • An encryption algorithm used to encrypt data traffic. Options are **3des**, **aes-128**, **aes-192**, **aes-256**, and **des**.

 Copyright © 2011, Juniper Networks, Inc.

Table 109: show security group-vpn member ipsec security-associations *(continued)*

Field Name	Field Description
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI.
Life: sec/kb	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.
GId	Group identifier.
vsys or Virtual-system	The root system.
Local Gateway	Gateway address of the local system.
GDOI Server	IP address of the group server.
Local Identity	Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IPv4 address, fully qualified domain name, e-mail address, or distinguished name.
Remote Identity	IPv4 address of the destination peer gateway.
DF-bit	State of the don't fragment bit: set or cleared.
Policy name	Name of the applicable policy.
Direction	Direction of the security association; it can be inbound or outbound.
AUX-SPI	Value of the auxiliary security parameter index. • When the value is AH or ESP, AUX-SPI is always 0. • When the value is AH+ESP, AUX-SPI is always a positive integer.
Hard lifetime	The hard lifetime specifies the lifetime of the SA. • **Expires in seconds**—Number of seconds left until the SA expires.
Lifesize Remaining	The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited. • **Expires in kilobytes**—Number of kilobytes left until the SA expires.
Soft lifetime	The soft lifetime informs the IPsec key management system that the SA is about to expire. Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. This allows the key management system to negotiate a new SA before the hard lifetime expires. • **Expires in seconds**—Number of seconds left until the SA expires.
Mode	Mode of the security association: • transport—Protects host-to-host connections. • tunnel—Protects connections between security gateways.

Copyright © 2011, Juniper Networks, Inc.

Table 109: show security group-vpn member ipsec security-associations *(continued)*

Field Name	Field Description
Protocol	Protocol supported. Transport mode supports Encapsulation Security Protocol (ESP).
Anti-replay service	State of the service that prevents packets from being replayed. It can be **Enabled** or **Disabled**.

show security group-vpn member ipsec security-associations

```
user@host> show security group-vpn member ipsec security-associations
  Total active tunnels: 1
  ID    Server           Port  Algorithm       SPI      Life:sec/kb  GId vsys
  >133955585 10.1.1.11   848   ESP:3des/sha1   d1d5e67d 587/  unlim   2   root
  <133955585 10.1.1.11   848   ESP:3des/sha1   d1d5e67d 587/  unlim   2   root
```

show security group-vpn member ipsec security-associations detail

```
user@host> show security group-vpn member ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 10.1.1.28, GDOI Server: 10.1.1.37
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Policy-name: p5-0001

    Direction: outbound, SPI: 68df21cc, AUX-SPI: 0, Group Id: 2
    Hard lifetime: Expires in 546 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 516 seconds
    Mode: shared, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: time-based enabled, Replay window size: 100

    Direction: inbound, SPI: 68df21cc, AUX-SPI: 0, Group Id: 2
    Hard lifetime: Expires in 546 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 516 seconds
    Mode: shared, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: time-based enabled, Replay window size: 100
```


Copyright © 2011, Juniper Networks, Inc.

show security group-vpn member kek security-associations

Syntax show security group-vpn member kek security-associations [brief | detail] [index *sa-index*] [*peer-ipaddress*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display group VPN security associations (SAs) for a group member.

Options none—Display information about all group VPN SAs for the group member.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed output.

index *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

peer-ipaddress—(Optional) Display information about the SA with the specified peer.

Required Privilege Level view

Related Documentation

- **clear security group-vpn member kek security-associations on page 1055**

List of Sample Output **show security group-vpn member kek security-associations on page 1425**
show security group-vpn member kek security-associations detail on page 1425

Output Fields Table 110 on page 1423 lists the output fields for the **show security group-vpn member kek security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 110: show security group-vpn member kek security-associations

Field Name	Field Description
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Remote Address	IP address of the destination peer with which the local peer communicates.
State	State of the KEK security associations: • **DOWN**—SA is not active. • **UP**—SA is active.
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.

Copyright © 2011, Juniper Networks, Inc.

Table 110: show security group-vpn member kek security-associations *(continued)*

Field Name	Field Description
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI.
GroupID	Group identifier.
KEK Peer	IP address of the destination peer with which the local peer communicates.
Role	For the member, it is always responder.
State	State of the KEK security associations, which is always up.
Authentication method	RSA is the supported authentication method.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Algorithms	Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:
	• **Sig-hash**—Type of authentication algorithm used.
	  ◦ **sha1**—Secure Hash Algorithm 1(sha1) authentication.
	  ◦ **md5**—MD5 authentication.
	• **Encryption**—Type of encryption algorithm used.
	  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.
	  ◦ **aes-192-cbc**— AES192-bit encryption
	  ◦ **aes-128-cbc**—AES 128-bit encryption.
	  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.
	  ◦ **des-cbc**—DES encryption.

Traffic statistics	• **Input bytes—**Number of bytes received. • **Output bytes—**Number of bytes transmitted. • **Input packets—**Number of packets received. • **Output packets—**Number of packets transmitted.
Server Info Version	Identify the latest set of information maintained in the server.
Server Heartbeat Interval	Interval in seconds at which the server sends heartbeats to group members.
Member Heartbeat Threshold	The heartbeat threshold configured on the group member for the IPsec VPN. If this number of heartbeats is missed on the member, the member reregisters with the server.
Heartbeat Timeout Left	Number of heartbeats until the heartbeat threshold is reached, at which time the member reregisters with the server. NOTE: When this number reaches 0, reregistration happens within 60 seconds.

Copyright © 2011, Juniper Networks, Inc.

Table 110: show security group-vpn member kek security-associations *(continued)*

Field Name	Field Description
Server Activation Delay	Number of seconds before a group member can use a new key when the member reregisters with the server.
Server Multicast Group	Multicast IP address to which the server sends rekey messages.
Server Replay Window	Antireplay time window value in seconds. 0 means antireplay is disabled.
Group Key Push sequence number	Sequence number of the KEK SA groupkey-push message. This number is incremented with every groupkey-push message, including heartbeats.

show security group-vpn member kek security-associations

```
user@host> show security group-vpn member kek security-associations
  Index   Remote Address  State  Initiator cookie  Responder cookie  GroupId
42      10.1.1.11       UP     a53603e30716fb74  8076194a850d56d0  2
```

show security group-vpn member kek security-associations detail

```
user@host> show security group-vpn member kek security-associations detail
KEK peer 10.1.1.37, Index 277
  Role: Responder, State: UP
  Initiator cookie: d858215649fba214, Responder cookie: e2ebd3fff04cf9d2
  Authentication method: RSA
  Local: 10.1.1.28:848, Remote: 10.1.1.37:848
  Lifetime: Expires in 37 seconds
  Algorithms:
   Sig-hash              : sha1
   Encryption            : 3des-cbc
  Traffic statistics:
   Input  bytes  :                  748
   Output bytes  :                   68
   Input  packets:                    3
   Output packets:                    1
  Group Id: 2
  Server Info Version: 5
  Server Heartbeat Interval: 60, Member Heartbeat Threshold: 5
  Heartbeat Timeout Left: 5
  Server Activation Delay: 10
  Server Multicast Group: Unicast, Server Replay Window: 100
  Group Key Push sequence number: 5
```

Copyright © 2011, Juniper Networks, Inc.

show security group-vpn server ike security-associations

Syntax show security group-vpn server ike security-associations [brief | detail] [group *group-name* | group-id *group-id*] [index *sa-index*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display IKE security associations (SAs).

Options none—Display all IKE SAs for all groups.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed level of output.

group—(Optional) Display IKE SAs for the specified group.

group-id—(Optional) Display IKE SAs for the specified group.

NOTE: An IKE SA can be used by a group member to register to multiple groups. When you specify the **group** or **group-id** options to list the IKE SAs for a specified group, all existing IKE SAs that could be used to register to the group are displayed.

index—(Optional) Display information for a particular SA based on the index number of the SA. To obtain the index number for a particular SA, display the list of existing SAs by using the command with no options.

Required Privilege Level view

Related Documentation

- **show security group-vpn member ike security-associations on page 1416**

List of Sample Output **show security group-vpn server ike security-associations on page 1428**
show security group-vpn server ike security-associations detail on page 1428

Output Fields Table 111 on page 1426 lists the output fields for the **show security group-vpn server ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 111: show security group-vpn member ike security-associations Output Fields

Field Name	Field Description
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Remote Address	IP address of the destination peer with which the local peer communicates.

 Copyright © 2011, Juniper Networks, Inc.

Table 111: show security group-vpn member ike security-associations Output Fields *(continued)*

Field Name	Field Description
State	State of the IKE security associations: • **DOWN**—SA has not been negotiated with the peer. • **UP**—SA has been negotiated with the peer.
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.
Mode	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are • **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
IKE Peer	IP address of the destination peer with which the local peer communicates.
Exchange type	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are • **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
Authentication method	Method the server uses to authenticate the source of IKE messages: • **pre-shared-keys**—Preshared key for encryption and decryption that both participants must have before beginning tunnel negotiations. **rsa-signatures**—Digital signature, a certificate that confirms the identity of the certificate holder.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Copyright © 2011, Juniper Networks, Inc.

Table 111: show security group-vpn member ike security-associations Output Fields *(continued)*

Field Name	Field Description

Algorithms	Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:
	• **Authentication**—Type of authentication algorithm used.
	  • **sha1**—Secure Hash Algorithm 1(sha1) authentication.
	  • **md5**—MD5 authentication.
	• **Encryption**—Type of encryption algorithm used.
	  • **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.
	  • **aes-192-cbc**— AES192-bit encryption
	  • **aes-128-cbc**—AES 128-bit encryption.
	  • **3des-cbc**—3 Data Encryption Standard (DES) encryption.
	  • **des-cbc**—DES encryption.

Traffic statistics	• **Input bytes—**Number of bytes received. • **Output bytes—**Number of bytes transmitted. • **Input packets—**Number of packets received. • **Output packets—**Number of packets transmitted.
IPSec security associations	• ***number* created:** The number of SAs created. • ***number* deleted**: The number of SAs deleted.

Phase 2 negotiations in progress	Number of Phase 2 IKE negotiations in progress and status information:
	• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.
	• **Message ID**—Unique identifier for a Phase 2 negotiation.
	• **Local identity**—Identity of the local Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)
	• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)
	• **Flags**—Notification to the key management process of the status of the IKE negotiation:
	  • **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.

show security group-vpn server ike security-associations

```
user@host> show security group-vpn server ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
2059    10.1.1.13       UP     86c09e79d3f986b6  aadaaaf97129b8cc  Main
```

show security group-vpn server ike

```
user@host> show security group-vpn server ike security-associations detail
IKE peer 10.1.1.13, Index 2059,
  Role: Responder, State: UP
```


Copyright © 2011, Juniper Networks, Inc.

security-associations detail

```
Initiator cookie: 86c09e79d3f986b6, Responder cookie: aadaaaf97129b8cc
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.1.11:848, Remote: 10.1.1.13:848
Lifetime: Expires in 3571 seconds
Algorithms:
 Authentication        : sha1
 Encryption            : 3des-cbc
 Pseudo random function: hmac-sha1
Traffic statistics:
 Input  bytes  :                  628
 Output bytes  :                 1196
 Input  packets:                    5
 Output packets:                    5
Flags: Caller notification sent
IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

  Negotiation type: Quick mode, Role: Responder, Message ID: 2158764791
  Local: 10.1.1.11:848, Remote: 10.1.1.13:848
  Local identity: 10.1.1.11
  Remote identity: 10.1.1.13
  Flags: Caller notification sent, Waiting for done
```

show security group-vpn server ipsec security-associations

Syntax show security group-vpn server ipsec security-associations [brief | detail] [group *group-name* | group-id *group-id*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display IPsec security associations (SAs).

Options none—Display all IPsec SAs for all groups.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed level of output.

group—(Optional) Display IPsec SAs for the specified group.

group-id—(Optional) Display IPsec SAs for the specified group.

Required Privilege Level view

Related Documentation

- Table 109 on page 1420

List of Sample Output **show security group-vpn server ipsec security-associations on page 1431**
show security group-vpn server ipsec security-associations detail on page 1431

Output Fields Table 112 on page 1430 lists the output fields for the **show security group-vpn server ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 112: show security group-vpn server ipsec security-associations

Field Name	Field Description
Group	Group name.
Group ID	Group identifier.
Total IPsec SAs	The total number of IPsec SAs for each group is shown.
IPsec SA	Name of the SA.
Protocol	Protocol supported. Transport mode supports Encapsulation Security Protocol (ESP).
Algorithm	Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes • An authentication algorithm used to authenticate exchanges between the peers. Options are **sha1** and **md5**. • An encryption algorithm used to encrypt data traffic. Options are **3des**, **aes-128**, **aes-192**, **aes-256**, or **des**.

 Copyright © 2011, Juniper Networks, Inc.

Table 112: show security group-vpn server ipsec security-associations *(continued)*

Field Name	Field Description
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI.
Lifetime	The lifetime of the SA, after which it expires, expressed in seconds.
Policy Name	Group policy associated with the IPsec SA. The source address, destination address, source port, destination port, and protocol defined for the policy are displayed.

show security group-vpn server ipsec security-associations

```
user@host> show security group-vpn server ipsec security-associations
Group: g2, Group Id: 2
  Total IPsec SAs: 2
  IPsec SA          Algorithm        SPI              Lifetime
  g2-gsa-1          ESP:aes-256/sha1 91f16f54         66
  g2-gsa-1          ESP:3des/sha1    39f8604a         1798
  g2-gsa-2          ESP:aes-256/sha1 e9450698         66
  g2-gsa-2          ESP:3des/sha1    99e3ead9         1798
Group: g3, Group Id: 3
  Total IPsec SAs: 2
  IPsec SA          Algorithm        SPI              Lifetime
  g2-gsa-1          ESP:aes-256/sha1 c81b4eba         66
  g2-gsa-1          ESP:3des/sha1    6696c219         1798
  g2-gsa-2          ESP:aes-256/sha1 e9230079         66
  g2-gsa-2          ESP:3des/sha1    710a231f         1798
```

In the output shown above, note that the encapsulation algorithm for the IPsec SAs changed from aes-256 to 3des. When this happened, the lifetime of the old key was reduced and the lifetime of the new key was set to 1800 seconds. When the **show** command was executed, 2 seconds had passed; therefore, the lifetime shown for the new keys is 1798 seconds.

show security group-vpn server ipsec security-associations detail

```
user@host> show security group-vpn server ipsec security-associations detail
Group: g2, Group Id: 2
Total IPsec SAs: 2
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: 91f16f54
    Lifetime left: 52
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 39f8604a
    Lifetime left: 1784
    Policy Name: gsa-pol-1
```

```
        Source: 0.0.0.0/0
        Destination: 1.1.2.0/24
        Source Port: 5
        Destination Port: 0
        Protocol: 0
      Policy Name: gsa-pol-2
        Source: 0.0.0.0/0
        Destination: 2.1.2.0/24
        Source Port: 5
        Destination Port: 0
        Protocol: 0
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: e9450698
    Lifetime left: 52
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 99e3ead9
    Lifetime left: 1784
Group: g3, Group Id: 3
Total IPsec SAs: 2
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: c81b4eba
    Lifetime left: 52
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 6696c219
    Lifetime left: 1784
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: e9230079
    Lifetime left: 52
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: 3des
```

 Copyright © 2011, Juniper Networks, Inc.

```
SPI: 710a231f
Lifetime left: 1784
```

show security group-vpn server kek security-associations

Syntax show security group-vpn server kek security-associations [brief | detail] [group *group-name* | group-id *group-id* | index *sa-index*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display configured server-member communications.

Options none—Display server-member communications configured for all groups.

brief—(Optional) Display summary output.

detail—(Optional) Display detailed output.

group—(Optional) Display server-member communications configured for the specified group.

group-id—(Optional) Display server-member communications configured for the specified group.

index—(Optional) Display information for a particular SA based on the index number of the SA. To obtain the index number for a particular SA, display the list of existing SAs by using the command with no options.

Required Privilege Level view

Related Documentation

- **show security group-vpn member kek security-associations on page 1423**

List of Sample Output **show security group-vpn server kek security-associations on page 1436**
show security group-vpn server kek security-associations detail on page 1436

Output Fields Table 113 on page 1434 lists the output fields for the **show security group-vpn server kek security-assocations** command. Output fields are listed in the approximate order in which they appear.

Table 113: show security group-vpn server kek security-associations Output Fields

Field Name	Field Description
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Remote Address	Identifier of the remote/peer. Because there could be multiple members, the remote address always contains the IP address 0.0.0.0.
State	State of the KEK security associations: • **DOWN**—SA is not active. • **UP**—SA is active.

 Copyright © 2011, Juniper Networks, Inc.

Table 113: show security group-vpn server kek security-associations Output Fields *(continued)*

Field Name	Field Description
Initiator cookie	Random number generated by the server. This is used when the server needs to push data to a member or send heartbeats to a member, or a member needs to reply to the server.
Responder cookie	Random number generated by the server. This is used when the server needs to push data to a member or send heartbeats to a member, or a member needs to reply to the server.
GroupId	Group identifier.
KEK Peer	IP address of the destination peer with which the local peer communicates. For KEK SAs, it always contains 0.0.0.0 which means any IP address.
Role	For the server, it is always initiator.
Authentication method	RSA is the supported authentication method.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Algorithms	Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the Phase 2 process:
	• **Sig-hash**—Type of authentication algorithm used.
	  ◦ **sha1**—Secure Hash Algorithm 1(sha1) authentication.
	  ◦ **md5**—MD5 authentication.
	• **Encryption**—Type of encryption algorithm used.
	  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.
	  ◦ **aes-192-cbc**— AES192-bit encryption
	  ◦ **aes-128-cbc**—AES 128-bit encryption.
	  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.
	  ◦ **des-cbc**—DES encryption.

Traffic statistics	• **Input bytes—**Number of bytes received. • **Output bytes—**Number of bytes transmitted. • **Input packets—**Number of packets received. • **Output packets—**Number of packets transmitted.
Server Info Version	Identify the latest set of information maintained in the server.
The following fields are the configured **server-member-communication** options:	
Server Heartbeat Interval	Interval in seconds at which the server sends heartbeats to group members.

Table 113: show security group-vpn server kek security-associations Output Fields *(continued)*

Field Name	Field Description
Server Activation Delay	Number of seconds before a group member can use a new key when the member reregisters with the server.
Server Multicast Group	Multicast IP address to which the server sends rekey messages.
Server Replay Window	Antireplay time in seconds. This is 0 if antireplay is disabled.
Retransmission Period	Number of seconds between a rekey transmission and the first retransmission when there is no reply from the member.
Number of Retransmissions	For unicast communications, the number of times the server retransmits rekey messages to a member when there is no reply. For multicast communications, the number of copies of a message the server sends to members.
Lifetime Seconds	Configured lifetime, in seconds, for the KEK.
Group Key Push sequence number	Sequence number of the KEK SA groupkey-push message. This number is incremented with every groupkey-push message, including heartbeats.

show security group-vpn server kek security-associations

```
user@host> show security group-vpn server kek security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  GroupId
2051    0.0.0.0         UP     e3ead57303ae393d  d97290c9a91b6a2a  2
2052    0.0.0.0         UP     39985f6e9878d4fe  8ad3cabd99918841  3
```

show security group-vpn server kek security-associations detail

```
user@host> show security group-vpn server kek security-associations detail
KEK peer 0.0.0.0, Index 2051
  Role: Initiator, State: UP
  Initiator cookie: e3ead57303ae393d, Responder cookie: d97290c9a91b6a2a
  Authentication method: RSA
  Local: 10.1.1.11:848, Remote: 0.0.0.0:848
  Lifetime: Expires in 934 seconds
  Algorithms:
   Sig-hash              : sha1
   Encryption            : 3des-cbc
  Traffic statistics:
   Input  bytes  :                   0
   Output bytes  :                2652
   Input  packets:                   0
   Output packets:                  13
  Group Id: 2, Group Name: g2
  Server Info Version: 135
  Server Heartbeat Interval: 60
  Server Activation Delay: 17
  Server Multicast Group: Unicast, Server Replay Window: 100
  Retransmission Period: 4, Number of Retransmissions: 2
  Lifetime Seconds: 1800
  Group Key Push sequence number: 13

KEK peer 0.0.0.0, Index 2052
  Role: Initiator, State: UP
  Initiator cookie: 39985f6e9878d4fe, Responder cookie: 8ad3cabd99918841
  Authentication method: RSA
```


Copyright © 2011, Juniper Networks, Inc.

```
Local: 10.1.1.11:848, Remote: 0.0.0.0:848
Lifetime: Expires in 934 seconds
Algorithms:
 Sig-hash              : sha1
 Encryption            : 3des-cbc
Traffic statistics:
 Input  bytes  :                    0
 Output bytes  :                    0
 Input  packets:                    0
 Output packets:                    0
Group Id: 3, Group Name: g3
Server Info Version: 135
Server Heartbeat Interval: 60
Server Activation Delay: 17
Server Multicast Group: Unicast, Server Replay Window: 100
Retransmission Period: 4, Number of Retransmissions: 2
Lifetime Seconds: 1800
Group Key Push sequence number: 0
```

show security group-vpn server registered-members

Syntax show security group-vpn server registered-members [group *group-name* | group-id *group-id*]

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display currently registered group members.

Options none—Display all group members for all groups.

group—(Optional) Display group members for the specified group.

group-id—(Optional) Display group members for the specified group.

Required Privilege Level view

Related Documentation

- **clear security group-vpn server on page 1056**

List of Sample Output **show security group-vpn server registered-members on page 1438**

Output Fields Table 114 on page 1438 lists the output fields for the **show security group-vpn server registered-members**command. Output fields are listed in the approximate order in which they appear.

Table 114: show security group—vpn server registered-members Output Fields

Field Name	Field Description
Group	Group name.
Group Id	Group identifier.
Member Gateway	IP address of the gateway for the group member.
Member IP	IP address of the group member.
Last Update	The last time that members registered or sent acknowledgements to the server.
Vsys	The root system.

show security group-vpn server registered-members

```
user@host> show security group-vpn server registered-members
Group: GroupA, Group Id: 1
  Member Gateway    Member IP   Last Update              Vsys
  gw-dn1            10.1.1.13   Tue Oct 20 2009 17:41:56 root
  gw-dn2            10.1.1.14   Tue Oct 20 2009 17:43:03 root


Group: GroupB, Group Id: 2
  Member Gateway    Member IP   Last Update              Vsys
  gw-enterprise     10.1.1.15   Tue Oct 20 2009 17:43:50 root
```

 Copyright © 2011, Juniper Networks, Inc.

show security idp active-policy

Syntax show security idp active-policy

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display information about the policy name and running detector version with which the policy is compiled from IDP data plane module.

Required Privilege Level view

Related Documentation

- **request security idp security-package download on page 1105**
- **request security idp security-package install on page 1107**

List of Sample Output **show security idp active-policy on page 1440**

Output Fields Table 115 on page 1440 lists the output fields for the **show security idp active-policy** command. Output fields are listed in the approximate order in which they appear.

Table 115: show security idp active-policy Output Fields

Field Name	Field Description
Policy Name	Name of the running policy.
Running Detector Version	Current version of the running detector.

show security idp active-policy

```
user@host> show security idp active-policy
  Policy Name : viking-policy
  Running Detector Version : 9.1.140080300
```


Copyright © 2011, Juniper Networks, Inc.

show security idp application-ddos application

Syntax show security idp application-ddos application

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display basic statistics for the servers being protected by the IDP application–level DDoS feature.

Options ***application–name*** —Display information on a specific application-level DDoS application profile.

context—Name of the application context for *application–name*

detail—Display a detailed view of the protected servers.

server—IP address of protected server.

zone—Zone name where the protected server resides.

Required Privilege Level view

List of Sample Output **show security idp application-ddos application on page 1441**
show security idp application-ddos application detail on page 1442

Output Fields Table 116 on page 1441 lists the output fields for the **show security idp application-ddos application** command.

Table 116: show security idp application-ddos Output Fields

Field Name	Field Description
Zone	Security zone where the protected server resides.
Server	IP address of the protected server.
Application	Name of the application-level DDoS application.
Conn/sec	Number of client connections to the protected server.
Context	Protocol context that is being monitored.
Contexts/tick	Number of protocol context hits measured per tick. One tick equals 60 seconds by default.

show security idp application-ddos application

```
user@host> show security idp application-ddos application

Zone    Server      Application     Conn/sec    Context                 Contexts/tick
trust   81.0.3.1    http-server-1   2648/sec    http-header-user-agent    35746/60sec
trust   81.1.0.2    dns-server-1    4517/sec    dns-type-name            263234/60sec
trust   81.1.0.2    dns-server-1    1497/sec    dns-type-name             88061/60sec
trust   81.0.3.1    http-server1    1496/sec    http-url-parsed           81177/60sec
```

Copyright © 2011, Juniper Networks, Inc.

```
...
```

show security idp application-ddos application detail

```
user@host> show security idp counters application-ddos detail

Zone: trust Server: 81.1.0.2 Application: dns-server-1 Connections/sec:
1499/secContext: dns-type-name Contexts/tick: 88061/60sec
Value: 00 05 74 65 73 74 6e 61 6d 65 2e 6a 75 6e 69 70 testname.juniper.net
Value: 65 72 2e 6e 65 74
Context values/tick : 29143/60sec

Zone: trust Server: 81.0.3.1 Application: http-server-1 Connections/sec:
2615/secContext: http-url contexts/tick: 148196/60sec
Value: 2f 6e 65 74 73 63 72 65 65 6e 2e 68 746d 6c /netscreen.htm
Context values/tick : 26809/60sec

...
```


Copyright © 2011, Juniper Networks, Inc.

show security idp application-identification application-system-cache

Syntax show security idp application-identification application-system-cache

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display application ID from the default port/protocol binding or from the application system cache.

Required Privilege Level view

Related Documentation
- **application-system-cache on page 349**
- **clear security idp application-identification application-system-cache on page 1058**

List of Sample Output **show security idp application-identification application-system-cache on page 1443**

Output Fields Table 117 on page 1443 lists the output fields for the **show security idp application-identification application-system-cache** command. Output fields are listed in the approximate order in which they appear.

Table 117: show security idp application-identification application-system-cache Output Fields

Field Name	Field Description
Vsys-ID	Application identification number.
IP address	IP address.
Port	Port number used with the current session.
Protocol	Name of the protocol session.
Expired	Session expired status: Yes or No
Service	Name of the service.

show security idp application-identification application-system-cache

```
user@host> show security idp application-identification application-system-cache
IDP Application System Cache statistics:
Vsys-ID     IP address        Port     Protocol  Expired  Service
  0           5.0.0.1          80       tcp       No         HTTP
  0         xxxx:xxxx::yyyy    2121     tcp                   FTP
```

show security idp attack table

Syntax show security idp attack table

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display detailed information of IDP attack table.

Required Privilege Level view

Related Documentation
- **clear security idp attack table on page 1059**

List of Sample Output **show security idp attack table on page 1444**

Output Fields Table 118 on page 1444 lists the output fields for the **show security idp attack table** command. Output fields are listed in the approximate order in which they appear.

Table 118: show security idp attack table Output Fields

Field Name	Field Description
Attack name	Name of the attack that you want to match in the monitored network traffic.
Hits	Total number of attack matches.

show security idp attack table

```
user@host> show security idp attack table
IDP attack statistics:
  Attack name                                   #Hits
  HTTP:OVERFLOW:PI3WEB-SLASH-OF                 1
```


Copyright © 2011, Juniper Networks, Inc.

show security idp counters application-ddos

Syntax show security idp counters application-ddos

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display the status of all IDP application-ddos counter values.

Required Privilege Level view

List of Sample Output **show security idp counters application-ddos on page 1446**

Output Fields Table 119 on page 1445 lists the output fields for the **show security idp counters application-ddos** command. Output fields are listed in the approximate order in which they appear.

Table 119: show security idp counters application-ddos Output Fields

Field Name	Field Description
App-DDOS inspected flows	Number of client-to-server flows inspected for application-ddos.
App-DDOS failed flows	Number of client-to-server flows that failed during application-ddos processing.
App-DDOS ignored flows	Number of client-to-server flows ignored for application-ddos.
App-DDOS first path failed	Number of client-to-server flow initialization failures during first path.
App-DDOS first path succeeded	Number of successful client-to-server flow initialization during first path.
App-DDOS dropped packets	Number of packets dropped in the application-level DDoS module.
App-DDOS processed packets	Number of total packets processed in the application-level DDoS module.
App-DDOS connection table process succeeded	Number of times connection processing succeeded.
App-DDOS connection table process failed	Number of times connection processing failed.
App-DDOS context process succeeded	Number of times the context processing succeeded.
App-DDOS context process failed	Number of times context processing failed.
App-DDOS ignore context	Number of contexts ignored if the flow is not client-to-server or if the application-level DDoS module is disabled.
App-DDOS context values excluded	Number of context values excluded for actions, reporting, or both.

Copyright © 2011, Juniper Networks, Inc.

Table 119: show security idp counters application-ddos Output Fields *(continued)*

Field Name	Field Description
App-DDOS context value process succeeded	Number of times context value processing succeeded, including action and logging events if configured.
App-DDOS context value process failed	Number of times context value processing failed, including action and logging events if configured.
App-DDOS context value prune failed	Number of times context value pruning failed.
App-DDOS no action	Number of times an attack is detected and no action is taken.
App-DDOS drop connection action	Number of times an attack is detected and a drop connection action is taken.
App-DDOS drop packet action	Number of times an attack is detected and a drop packet action is taken.
App-DDOS close server action	Number of times an attack is detected and a close server action is taken.
App-DDOS IP Action block	Number of times an ip-action block entry is created and installed.
App-DDOS IP Action close	Number of times an ip-action close entry is created and installed.
App-DDOS Action notify	Number of times an ip-action notify entry is created and installed.
App-DDOS logs sent	Number of attack logs sent.
App-DDOS logs report failed	Number of attack log reports that failed.

show security idp counters application-ddos

```
user@host> show security idp counters application-ddos

 App-DDOS inspected flows                                    447172
 App-DDOS failed flows                                       0
 App-DDOS ignored flows                                      12267
 App-DDOS first path failed                                  0
 App-DDOS first path succeeded                               459439
 App-DDOS dropped packets                                    0
 App-DDOS processed packets                                  449118
 App-DDOS connection table process succeeded                 459439
 App-DDOS connection table process failed                    0
 App-DDOS context process succeeded                          449118
 App-DDOS context process failed                             0
 App-DDOS ignore context                                     0
 App-DDOS context values excluded                            0
 App-DDOS context value process succeeded                    449118
 App-DDOS context value process failed                       0
 App-DDOS context value prune failed                         0
 App-DDOS no action                                          275996
 App-DDOS drop connection action                             0
 App-DDOS drop packet action                                 0
 App-DDOS close server action                                0
 App-DDOS IP Action block                                    0
 App-DDOS IP Action close                                    0
 App-DDOS IP Action notify                                   275996
```


Copyright © 2011, Juniper Networks, Inc.

```
App-DDOS logs sent                                          238
App-DDOS logs report failed                                 0
```

show security idp counters application-identification

Syntax show security idp counters application-identification

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all IDP application identification (AI) counter values.

Required Privilege Level view

Related Documentation
- **application-identification on page 342**
- **clear security idp counters application-identification on page 1060**

List of Sample Output **show security idp counters application-identification on page 1449**

Output Fields Table 120 on page 1448 lists the output fields for the **show security idp counters application-identification** command. Output fields are listed in the approximate order in which they appear.

Table 120: show security idp counters application-identification Output Fields

Field Name	Field Description
AI cache hits	Number of sessions found application in AI cache.
AI cache misses	Number of sessions those did not find application from AI cache.
AI matches	Number of sessions matched AI signatures.
AI no-matches	Number of sessions that did not match AI signatures.
AI-enabled sessions	Number of sessions that are AI enabled.
AI-disabled sessions	Number of sessions that are AI disabled.
AI-disabled sessions due to gate match	Number of sessions disabled AI match due to gate match.
AI-disabled sessions due to ssl encapsulated flows	Number of sessions disabled AI match due to ssl encapsulated flows.
AI-disabled sessions due to cache hit	Number of sessions disabled AI match due to AI cache match.
AI-disabled sessions due to configuration	Number of sessions disabled AI match due to AI session limit in the configuration.
AI-disabled sessions due to protocol remapping	Number of sessions disabled AI match due to protocol remapping.

Copyright © 2011, Juniper Networks, Inc.

Table 120: show security idp counters application-identification Output Fields *(continued)*

Field Name	Field Description
AI-disabled sessions due to RPC match	Number of sessions disabled AI match due to RPC match.
AI-disabled sessions due to Aux/Dynamic/Encap/Mgmt flows (Unsupported)	Number of sessions disabled AI match due to auxiliary, dynamic, encapsulated, or management flows.
AI-disabled sessions due to non-TCP/UDP flows	Number of sessions disabled AI match due to non-TCP or non-UDP flows.
AI-disabled sessions due to no AI signatures (Unsupported)	Number of sessions disabled AI match due to absence of AI signature.
AI-disabled sessions due to session limit	Number of sessions disabled AI match after reaching AI max session limit.
AI-disabled sessions due to session packet memory limit	Number of sessions disabled AI match after reaching AI memory usage limit per session.
AI-disabled sessions due to global packet memory limit	Number of sessions disabled AI match after reaching AI global memory usage limit.

show security idp counters application-identification

```
user@host> show security idp counters application-identification
IDP counters:
IDP counter type                                                    Value
 AI cache hits                                                         2682
 AI cache misses                                                       3804
 AI matches                                                            74
 AI no-matches                                                         27
 AI-enabled sessions                                                   3804
 AI-disabled sessions                                                  2834
 AI-disabled sessions due to gate match                                0
 AI-disabled sessions due to ssl encapsulated flows                    0
 AI-disabled sessions due to cache hit                                 2682
 AI-disabled sessions due to configuration                             0
 AI-disabled sessions due to protocol remapping                        0
 AI-disabled sessions due to RPC match                                 0
 AI-disabled sessions due to Aux/Dynamic/Encap/Mgmt flows              0
 AI-disabled sessions due to non-TCP/UDP flows                         118
 AI-disabled sessions due to no AI signatures                          0
 AI-disabled sessions due to session limit                             0
 AI-disabled sessions due to session packet memory limit               34
 AI-disabled sessions due to global packet memory limit                0
```

show security idp counters dfa

Syntax show security idp counters dfa

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all DFA counter values.

Required Privilege Level view

Related Documentation
- **clear security idp counters dfa on page 1061**

List of Sample Output **show security idp counters dfa on page 1450**

Output Fields Table 121 on page 1450 lists the output fields for the **show security idp counters dfa** command. Output fields are listed in the approximate order in which they appear.

Table 121: show security idp counters dfa Output Fields

Field Name	Field Description
DFA Group Merged Usage	Number of DFA groups merged.
DFA Matches	Number of DFA matches found.

show security idp counters dfa

```
user@host> show security idp counters dfa
IDP counters:
IDP counter type                                                    Value
 DFA Group Merged Usage                                               0
 DFA Matches                                                          1
```

 Copyright © 2011, Juniper Networks, Inc.

show security idp counters flow

Syntax show security idp counters flow

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all IDP flow counter values.

Required Privilege Level view

Related Documentation
- **flow (IDP) on page 457**
- **clear security idp counters flow on page 1062**

List of Sample Output **show security idp counters flow on page 1452**

Output Fields Table 122 on page 1451 lists the output fields for the **show security idp counters flow** command. Output fields are listed in the approximate order in which they appear.

Table 122: show security idp counters flow Output Fields

Field Name	Field Description
Fast-path packets	Number of packets that are set through fast path after completing idp policy lookup.
Slow-path packets	Number of packet that are sent through slow path during idp policy lookup.
ICMP-error packets (Unsupported)	Number of ICMP error packets.
Session construction failed (Unsupported)	Number of times the packet failed to establish the session.
Session limit reached	Number of sessions that reached idp sessions limit.
Not a new session (Unsupported)	Number of session that extended from its time limit.
Invalide index at ageout (Unsupported)	Invalid session index in session ageout message.
Packet logging	Number of packets saved for packet logging.
Busy packets (Unsupported)	Number of packets saved as the one or more packets of this session are handed off for async processing.
Policy cache hits	Number of sessions that matched policy cache.

Copyright © 2011, Juniper Networks, Inc.

Table 122: show security idp counters flow Output Fields *(continued)*

Field Name	Field Description
Policy cache misses	Number of sessions that did not match policy cache.
Maximum flow hash collisions	Maximum number of packets of one flow that share the same hash value.
Bad-UDP-checksumpackets (Unsupported)	Number of packets that received with bad UDP checksum error.
Gates added	Number of gate entries added for dynamic port identification.
Gate matches (Unsupported)	Number of times a gate is matched.
Sessions deleted	Number of sessions deleted.
Sessions aged-out (Unsupported)	Number of sessions are aged out if no traffic is received within session timeout value.
Sessions in-use while aged-out (Unsupported)	Number of sessions in use during session ageout.
TCP flows marked dead on RST/FIN	Number of session marked dead on TCP RST/FIN.
Sessions constructed	Number of sessions established.
Sessions destructed	Number of sessions destructed.
SM Session Create	Number of SM sessions created.
SM Session close	Number of SM sessions closed.

show security idp counters flow

```
user@host> show security idp counters flow
IDP counters:
 IDP counter type                                          Value
 Fast-path packets                                           0
 Slow-path packets                                           1
 ICMP-error packets                                          0
 Session construction failed                                 0
 Session limit reached                                       0
 Not a new session                                           0
 Invalide index at ageout                                    0
 Packet logging                                              0
 Busy packets                                                0
 Policy cache hits                                           0
 Policy cache misses                                         1
```


Copyright © 2011, Juniper Networks, Inc.

```
Maximum flow hash collisions                                    0
Flow hash collisions                                            0
Bad-UDP-checksum packets                                        0
Gates added                                                     0
Gate matches                                                    0
Sessions deleted                                                1
Sessions aged-out                                               0
Sessoins in-use while aged-out                                  0
TCP flows marked dead on RST/FIN                                1
Sessions constructed                                            1
Sessions destructed                                             1
SM Session Create                                               1
SM Packet Process                                               28
SM Session close                                                1
```

show security idp counters ips

Syntax show security idp counters ips

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all IPS counter values.

Required Privilege Level view

Related Documentation
- **ips on page 532**
- **clear security idp counters ips on page 1063**

List of Sample Output **show security idp counters ips on page 1455**

Output Fields Table 123 on page 1454 lists the output fields for the **show security idp counters ips** command. Output fields are listed in the approximate order in which they appear.

Table 123: show security idp counters ips Output Fields

Field Name	Field Description
TCP fast path	Number of TCP packets skipped for IDS processing.
Layer-4 anomalies	Number of Layer-4 protocol error or anomaly.
Anomaly hash misses	Number of times look failed on anomaly hash.
Line context matches	Number of attempts to match line based attacks in traffic stream.
Stream256 context matches	Number of attempts to match stream based attacks in first 256 bytes of traffic stream.
Stream context matches	Number of attempts to match stream based attacks in traffic stream.
Packet context matches	Number of attempts to match packet based attacks in traffic packet.
Packet header matches	Number of attempts to match packet header based attacks in traffic packet.
Context matches	Number of attempts to match protocol context based attacks in traffic stream.
Regular expression matches	Number of attempts to match PCRE expressions in traffic stream.
Tail DFAs	Number of attempts to match an attack on tail DFA group matches.
Exempted attacks	Number of attacks exempted from match as per exempt rulebase.
Out of order chains	Number of times attack is excluded from match due to member attacks in an attack group did not complete chain.

Copyright © 2011, Juniper Networks, Inc.

Table 123: show security idp counters ips Output Fields *(continued)*

Field Name	Field Description
Partial chain matches	Number of attacks in partial chain match with attack scope as transaction.
IDS device FIFO size	Number of IDS contexts in virtual IDS device.
IDS device FIFO overflows	Number of times an IDS context can not be written as the IDS device is full.
Brute force queue size	Number of entries in the brute force queue.
IDS cache hits (Unsupported)	Number of sessions those found attack instance in IDS cache.
IDS cache misses (Unsupported)	Number of sessions those did not find attack instance in IDS cache.
Shellcode detection invocations	Number of times shell code match is attempted.
Wrong offsets	Number of times attack's offset is not within the service offset range.
No peer MAC (Unsupported)	Number of times flow peer MAC address is not available.

show security idp counters ips

```
user@host> show security idp counters ips
IDP counters:
 IDP counter type                                                    Value
 TCP fast path                                                         15
 Layer-4 anomalies                                                      0
 Anomaly hash misses                                                    3
 Line context matches                                                   5
 Stream256 context matches                                              5
 Stream context matches                                                 5
 Packet context matches                                                 0
 Packet header matches                                                  0
 Context matches                                                       12
 Regular expression matches                                             0
 Tail DFAs                                                              0
 Exempted attacks                                                       0
 Out of order chains                                                    0
 Partial chain matches                                                  0
 IDS device FIFO size                                                   0
 IDS device FIFO overflows                                              0
 Brute force queue size                                                 0
 IDS cache hits                                                         0
 IDS cache misses                                                       0
 Shellcode detection invocations                                        0
 Wrong offsets                                                          0
 No peer MAC                                                            0
```

show security idp counters log

Syntax show security idp counters log

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all IDP log counter values.

Required Privilege Level view

Related Documentation
- **event-rate on page 435**
- **clear security idp counters log on page 1064**

List of Sample Output **show security idp counters log on page 1457**

Output Fields Table 124 on page 1456 lists the output fields for the **show security idp counters log** command. Output fields are listed in the approximate order in which they appear.

Table 124: show security idp counters log Output Fields

Field Name	Field Description
Logs dropped	Number of logs that are dropped.
Suppressed log count	Number of logs that are suppressed.
Logs waiting for post-window packets (Unsupported)	Number of logs waiting for post-window packets.
Logs ready to be sent (Unsupported)	Number of logs ready to be sent.
Logs in suppression list (Unsupported)	Number of logs considered for suppression list.
Log timers created	Number of times the log timer is created.
Logs timers expired	Number of times the log timer is expired.
Log timers cancelled	Number of times the log timer is canceled.
Logs ready to be sent high watermark (Unsupported)	Number of packets that are ready to be sent with high degree watermark.
Log receive buffer full (Unsupported)	Number of times the buffer is full.

Copyright © 2011, Juniper Networks, Inc.

Table 124: show security idp counters log Output Fields *(continued)*

Field Name	Field Description
Packet log too big (Unsupported)	Number of packet logs that exceeded allowed packet log size.
Reads per second (Unsupported)	Number of packets that are read per second.
Logs in read buffer high watermark (Unsupported)	Number of high watermark packets that are in read buffer.
Packets logged	Number of packets that are logged,
Packets lost (Unsupported)	Number of packets that are failed to log.
Packets copied (Unsupported)	Number of packets copied during packet log.
Packets held (Unsupported)	Number of packets held for packet log.
Packets released	Number of packets that are released from hold.
IP Action Messages (Unsupported)	Number of IP action messages.
IP Action Drops (Unsupported)	Number of IP action messages dropped.
IP Action Exists (Unsupported)	Number of exits during IP action creation.
NWaits (Unsupported)	Number of logs waiting for post window packets.
Match vectors	Number of attacks in IDS match vector.
Supercedes	Number of attacks in supercede vector.

show security idp counters log

```
user@host> show security idp counters log
IDP counters:
 IDP counter type                                                    Value
```

```
Logs dropped                                                    0
Suppressed log count                                            0
Logs waiting for post-window packets                            0
Logs ready to be sent                                           0
Logs in suppression list                                        0
Log timers created                                              0
Logs timers expired                                             0
Log timers cancelled                                            0
Logs ready to be sent high watermark                            0
Log receive buffer full                                         0
Packet log too big                                              0
Reads per second                                                1
Logs in read buffer high watermark                              0
Log Bytes in read buffer high watermark                         0
Packets logged                                                  0
Packets lost                                                    0
Packets copied                                                  0
Packets held                                                    0
Packets released                                                0
IP Action Messages                                              0
IP Action Drops                                                 0
IP Action Exists                                                0
NWaits                                                          0
Match vectors                                                   0
Supercedes                                                      0
Kpacket too big                                                 0
```


Copyright © 2011, Juniper Networks, Inc.

show security idp counters packet

Syntax show security idp counters packet

Release Information Command introduced in Release 9.2 of Junos OS. **Dropped by IDP policy** and **Dropped by Error** added in Release 10.1 of Junos OS.

Description Display the status of all IDP packet counter values.

Required Privilege Level view

Related Documentation

- **clear security idp counters packet on page 1065**

List of Sample Output **show security idp counters packet on page 1461**

Output Fields Table 125 on page 1459 lists the output fields for the **show security idp counters packet** command. Output fields are listed in the approximate order in which they appear.

Table 125: show security idp counters packet Output Fields

Field Name	Field Description
Processed packets	Number of packets processed by the IDP service.
Dropped packets	Number of packets dropped by the IDP service.
Dropped by IDP policy	Number of packets dropped by the IDP policy.
Dropped by Error	Number of packets dropped by error.
Dropped sessions (Unsupported)	Number of sessions dropped.
Bad IP headers	Number of packets that fail IP header length validity check.
Packets with IP options	Number of packets that contain the optional header fields.
Decapsulated packets	Number of packets that are decapsulated.
GRE decapsulations (Unsupported)	Number of packets that are generic routing encapsulation (GRE) decapsulated.
PPP decapsulations (Unsupported)	Number of packets that are Point-to-Point Protocol (PPP) decapsulated.
GTP decapsulations (Unsupported)	Number of packets that are GPRS tunneling protocol (GTP) decapsulated.

Copyright © 2011, Juniper Networks, Inc.

Table 125: show security idp counters packet Output Fields *(continued)*

Field Name	Field Description
GTP flows (Unsupported)	Number of GTP flows.
TCP decompression uncompressed IP (Unsupported)	Number of uncompressed IP headers that are to be TCP decompressed.
TCP decompression compressed IP (Unsupported)	Number of compressed IP headers that are to be TCP decompressed.
Deferred-send packets (Unsupported)	Number of deferred IP packets that are sent out.
IP-in-IP packets (Unsupported)	Number of packets that are IP-in-IP encapsulated.
TTL errors (Unsupported)	Number of packets with TTL error in the header.
Routing loops (Unsupported)	Number of packets that continue to be routed in an endless circle due to an inconsistent routing state.
No-route packets (Unsupported)	Number of packets that could not be routed further.
Flood IP (Unsupported)	Number of packets that are identified as IP flood packets.
Invalid ethernet headers (Unsupported)	Number of packets that are identified with an invalid Ethernet header.
Packets attached	Number of packets attached.
Packets cloned	Number of packets that are cloned.
Packets allocated	Number of packets allocated.
Packets destructed	Number of packets destructed.

Copyright © 2011, Juniper Networks, Inc.

show security idp counters packet

```
user@host> show security idp counters packet
IDP counters:
 IDP counter type                                                    Value
 Processed packets                                                     27
 Dropped packets                                                        0
 Dropped by IDP policy                                                  0
 Dropped by error                                                       0
 Dropped sessions                                                       0
 Bad IP headers                                                         0
 Packets with IP options                                                0
 Decapsulated packets                                                   0
 GRE decapsulations                                                     0
 PPP decapsulations                                                     0
 GTP decapsulations                                                     0
 GTP flows                                                              0
 TCP decompression uncompressed IP                                      0
 TCP decompression compressed IP                                        0
 Deferred-send packets                                                  0
 IP-in-IP packets                                                       0
 TTL errors                                                             0
 Routing loops                                                          0
 STP drops                                                              0
 No-route packets                                                       0
 Flood IP                                                               0
 Invalid ethernet headers                                               0
 Packets attached                                                      28
 Packets cloned                                                        28
 Packets allocated                                                      0
 Packets destructed                                                    55
```

show security idp counters packet-log

Syntax show security idp counters packet-log

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the values of all IDP packet-log counters.

Required Privilege Level view

Output Fields The following table lists the output fields for the **show security idp counters packet-log** command. Output fields are listed in the approximate order in which they appear.

Field Name	Field Description
Total packets captured since packet capture was activated	Number of packets captured by the device by the IDP service.
Total sessions enabled since packet capture was activated	Number of sessions that have performed packet capture since the capture facility was activated.
Sessions currently enabled for packet capture	Number of sessions that are actively capturing packets at this time.
Packets currently captured for enabled sessions	Number of packets that have been captured by active sessions.
Packet clone failures	Number of packet capture failures due to cloning error.
Session log object failures	Number of objects containing log messages generated during packet capture that were not successfully transmitted to the host.
Session packet log object failures	Number of objects containing captured packets that were not successfully transmitted to the host.
Sessions skipped because session limit exceeded	Number of sessions that could not initiate packet capture because the maximum number of sessions specified for the device were conducting captures at that time.
Packets skipped because packet limit exceeded	Number of packets not captured because the packet limit specified for this device was reached.
Packets skipped because total memory limit exceeded	Number of packets not captured because the memory allocated for packet capture on this device was exceeded.

show security idp counters packet-log

```
user@host> show security idp counters packet-log
IDP counters:                                                    Value
 Total packets captured since packet capture was activated           0
 Total sessions enabled since packet capture was activated           0
 Sessions currently enabled for packet capture                       0
 Packets currently captured for enabled sessions                     0
 Packet clone failures                                               0
```


Copyright © 2011, Juniper Networks, Inc.

```
Session log object failures                                    0
Session packet log object failures                             0
Sessions skipped because session limit exceeded                0
Packets skipped because packet limit exceeded                  0
Packets skipped because total memory limit exceeded            0
```

show security idp counters policy-manager

Syntax show security idp counters policy-manager

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all IDP policies counter values.

Required Privilege Level view

Related Documentation
- **clear security idp counters policy-manager on page 1066**

List of Sample Output **show security idp counters policy-manager on page 1464**

Output Fields Table 126 on page 1464 lists the output fields for the **show security idp counters policy-manager** command. Output fields are listed in the approximate order in which they appear.

Table 126: show security idp counters policy-manager Output Fields

Field Name	Field Description
Number of policies	Number of policies installed.
Number of aged out policies	Number of IDP policies that are expired.

show security idp counters policy-manager

```
user@host> show security idp counters policy-manager
IDP counters:
 IDP counter type                                                    Value
 Number of policies                                                    0
 Number of aged out policies                                           0
```

 Copyright © 2011, Juniper Networks, Inc.

show security idp counters tcp-reassembler

Syntax show security idp counters tcp-reassembler

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display the status of all TCP reassembler counter values.

Required Privilege Level view

Related Documentation

- **re-assembler on page 666**
- **clear security idp counters tcp-reassembler on page 1067**

List of Sample Output **show security idp counters tcp-reassembler on page 1466**

Output Fields Table 127 on page 1465 lists the output fields for the **show security idp counters tcp-reassembler** command. Output fields are listed in the approximate order in which they appear.

Table 127: show security idp counters tcp-reassembler Output Fields

Field Name	Field Description
Bad TCP checksums (Unsupported)	Number of packets that have incorrect TCP checksums.
Bad TCP headers	Number of bad TCP headers detected.
Slow path segments	Number of segments that are sent through the slow path if the TCP segment does not pass fast-path segment validation.
Fast path segments	Number of segments that are sent through the fast path after passing a predefined TCP validation sequence.
Sequence number wrap around errors	Number of packets that wrap around of the sequence number.
Session reuses	Number of sessions that reused an already established TCP session.
SYN retransmissions	Number of SYN packets that are retransmitted.
Bad three way handshake acknowledgements	Number of packets that have incorrect three-way handshake acknowledgements (ACK packet).
Sequence number out of sync flows	Number of packets that have out-of-sync sequence numbers.
Fast path pattern matches in queued up streams	Number of queued packets that have fast path pattern match.

Copyright © 2011, Juniper Networks, Inc.

Table 127: show security idp counters tcp-reassembler Output Fields *(continued)*

Field Name	Field Description
New segments with no overlaps with old segment	Number of new segments that do not overlap with old segment.
New segment overlaps with beginning of old segment	Number of new segments that overlap with beginning of old segment.
New segment overlaps completely with old segment	Number of new segments that overlap completely with old segment.
New segment is contained in old segment	Number of new segments contained in old segment.
New segment overlaps with end of old segment	Number of new segments that overlap with the end of old segment.
New segment begins after end of old segment	Number of new segments that overlap after the end of old segment.
Memory consumed by new segment	Memory that is consumed by the new segment.
Segments in memory	Number of segments that are stored in memory for processing.
Per-flow memory overflows	Number of segments dropped after reaching per flow memory limit.
Global memory overflows	Number of segments dropped after reaching reassembler global memory limit.
Overflow drops	Number of packets that are dropped due to memory overflow.
Copied packets (Unsupported)	Number of packets copied in reassembler.
Closed Acks	Number of Ack packets seen without having seen SYN on the same session.

show security idp counters tcp-reassembler

```
user@host> show security idp counters tcp-reassembler
IDP counters:
 IDP counter type                                                    Value
 Bad TCP checksums                                                     0
 Bad TCP headers                                                       0
 Slow path segments                                                    4
 Fast path segments                                                    23
 Sequence number wrap around errors                                    0
 Session reuses                                                        0
 SYN retransmissions                                                   0
 Bad three way handshake acknowledgements                              0
 Sequence number out of sync flows                                     0
 Fast path pattern matches in queued up streams                        0
 New segments with no overlaps with old segment                        0
 New segment overlaps with beginning of old segment                    0
 New segment overlaps completely with old segment                      0
```


Copyright © 2011, Juniper Networks, Inc.

```
New segment is contained in old segment                          0
New segment overlaps with end of old segment                     0
New segment begins after end of old segment                      0
Memory consumed by new segment                                   0
Segments in memory                                               0
Per-flow memory overflows                                        0
Global memory overflows                                          0
Overflow drops                                                   0
Copied packets                                                   0
Closed Acks                                                      0
```

show security idp memory

Syntax show security idp memory

Release Information Command introduced in Release 9.2 of Junos OS. Percentage outputs added in Release 10.1 of Junos OS.

Description Display the status of all IDP data plane memory.

Required Privilege Level view

List of Sample Output **show security idp memory on page 1468**

Output Fields Table 128 on page 1468 lists the output fields for the **show security idp memory** command. Output fields are listed in the approximate order in which they appear.

Table 128: show security idp memory Output Fields

Field Name	Field Description
PIC	Name of the PIC.
Total IDP data plane memory	Total memory space that is allocated for the IDP data plane.
Used	Used memory space in the data plane.
Available	Available memory space in the data plane.

show security idp memory

```
user@host> show security idp memory
    IDP data plane memory statistics:
                          PIC : FPC 0 PIC 0:
  Total IDP data plane memory : 196 MB
                         Used : 8 MB ( 8192 KB ) ( 4.08% )
                    Available : 188 MB ( 192512 KB ) (95.91%)
```


Copyright © 2011, Juniper Networks, Inc.

show security idp policies

Syntax show security idp policies

Release Information Command introduced in Release 10.1 of Junos OS.

Description Display the list of currently installed policies.

Required Privilege Level view

Related Documentation

- **show security idp active-policy on page 1440**

Output Fields **user@host> show security idp policies**

Sample Output

```
Subscriber:  s0,        Installed policies:  1

  ID     Name    Sessions    Memory    detector

  0      new1      0         10179       9.2.160090324
```

show security idp policy-templates

Syntax show security idp policy-templates

Release Information Command introduced in Release 10.1 of Junos OS.

Description Display the list of available policy templates.

Required Privilege Level view

Related Documentation

- **show security idp active-policy on page 1440**

Output Fields **user@host> show security idp policy-templates**

Sample Output

```
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Web_Server
```


Copyright © 2011, Juniper Networks, Inc.

show security idp predefined-attacks

Syntax

show security idp predefined-attacks
filters (category | severity | direction)

Release Information

Command introduced in Release 10.1 of Junos OS.

Description

Display information about predefined attacks using optional filters.

Options

filters (Optional)

- **category**—Show predefined attacks in different categories.
- **severity**—Show predefined attacks based on different severities.
  - **critical**
  - **info**
  - **major**
  - **minor**
  - **warning**
- **direction** — Show predefined attacks for different directions.
  - **any**
  - **client-to-server**
  - **exclude-any**
  - **exclude-client-to-server**
  - **exclude-server-to-client**
  - **server-to-client**

Required Privilege Level

view

Output Fields

user@host> show security idp predefined-attacks filters category APP

Sample Output

```
APP:AMANDA:AMANDA-ROOT-OF1
APP:AMANDA:AMANDA-ROOT-OF2
APP:ARKEIA:TYPE-77-OF
APP:CA:ALERT-SRV-OF
APP:CA:ARCSRV:TCP-BOF
APP:CA:ARCSRV:UA-OF
APP:CA:IGATEWAY-BOF
APP:CA:LIC-COMMAND-OF
APP:CA:LIC-GCR-OF
APP:CA:LIC-GETCONFIG-OF
APP:CA:LIC-GETCONFIG-OF2
APP:CA:LIC-PUTOLF-OF
```

Copyright © 2011, Juniper Networks, Inc.

```
APP:CDE-DTSPCD-OF
APP:DOUBLETAKE
APP:ETHEREAL:DISTCC-OF
APP:HPOVNNM:HPOVTRACE-OF
APP:KERBEROS:GSS-ZERO-TOKEN
APP:KERBEROS:KBR-DOS-TCP-2
APP:MDAEMON:FORM2RAW-OF
APP:MERCURY-BOF
APP:MISC:MCAFFEE-SRV-HDR
APP:NTOP-WEB-FS1
APP:PPTP:MICROSOFT-PPTP
APP:REMOTE:TIMBUKTU-AUTH-OF
```

user@host> show security idp security-package predefined-attacks filters category FTP severity critical direction client-to-server

```
FTP:COMMAND:WZ-SITE-EXEC
FTP:DIRECTORY:TILDE-ROOT
FTP:EXPLOIT:OPENFTPD-MSG-FS
FTP:OVERFLOW:OPENBSD-FTPD-GLOB
FTP:OVERFLOW:PATH-LINUX-X86-3
FTP:OVERFLOW:WFTPD-MKD-OVERFLOW
FTP:OVERFLOW:WUBSD-SE-RACE
FTP:PROFTP:OVERFLOW1
FTP:PROFTP:PPC-FS2
FTP:SERVU:CHMOD-OVERFLOW
FTP:SERVU:LIST-OVERFLOW
FTP:SERVU:MDTM-OVERFLOW
FTP:WU-FTP:IREPLY-FS
```


Copyright © 2011, Juniper Networks, Inc.

show security idp security-package-version

Syntax show security idp security-package-version

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display information of the currently installed security package version and detector version.

Required Privilege Level view

Related Documentation

- **security-package on page 703**
- **request security idp security-package download on page 1105**
- **request security idp security-package install on page 1107**

List of Sample Output **show security idp security-package-version on page 1473**

Output Fields Table 129 on page 1473 lists the output fields for the **show security idp security-package-version** command. Output fields are listed in the approximate order in which they appear.

Table 129: show security idp security-package-version Output Fields

Field Name	Field Description
Attack database version	Attack database version number that are currently installed on the system.
Detector version	Detector version number that are currently installed on the system.
Policy template version	Policy template version that are currently installed on the system.

show security idp security-package-version

```
user@host> show security idp security-package-version
  Attack database version:1154(Mon Apr 28 15:08:42 2008)
  Detector version :9.1.140080400
  Policy template version :7
```

show security idp ssl-inspection key

Syntax **show security idp ssl-inspection key** [*<key-name>* [**server** *<server-ip>*]]

Release Information Command introduced in Release 9.3 of Junos OS.

Description Display SSL keys added to the system along with their associated server IP addresses.

Options ***key-name*** —(Optional) Name of SSL private key.

server ***server-ip*** —(Optional) Server IP address associated for specified key.

Required Privilege Level view

List of Sample Output **show security idp ssl-inspection key on page 1474**
show security idp ssl-inspection key key2 on page 1474

Output Fields Table 130 on page 1474 lists the output fields for the **show security idp ssl-inspection key** command. Output fields are listed in the approximate order in which they appear.

Table 130: show security idp ssl-inspection key Output Fields

Field Name	Field Description
Total SSL keys	Total number of SSL keys.
key	Name of the SSL private key.
server	Server IP address associated with the SSL keys.

show security idp ssl-inspection key

```
user@host> show security idp ssl-inspection key
Total SSL keys : 4

SSL Server key and ip address:

  Key : key1, server : 1.1.0.1
  Key : key1, server : 1.1.0.2
  Key : key2, server : 2.2.0.1
  key : key3
```

show security idp ssl-inspection key key2

```
user@host> show security idp ssl-inspection key key2
SSL Server key and ip address:

  Key : key2, server : 2.2.0.1
```

 Copyright © 2011, Juniper Networks, Inc.

show security idp ssl-inspection session-id-cache

Syntax show security idp ssl-inspection session-id-cache

Release Information Command introduced in Release 9.3 of Junos OS.

Description Display all the SSL session IDs in the session ID cache. Each cache entry is 32 bytes long.

Required Privilege Level view

Related Documentation
- **clear security idp ssl-inspection session-id-cache on page 1068**

List of Sample Output **show security idp ssl-inspection session-id-cache on page 1475**

Output Fields Table 131 on page 1475 lists the output fields for the **show security idp ssl-inspection session-id-cache** command. Output fields are listed in the approximate order in which they appear.

Table 131: show security idp ssl-inspection session-id-cache Output Fields

Field Name	Field Description
Total SSL session identifiers	Total number of SSL session identifiers stored in the session ID cache.

show security idp ssl-inspection session-id-cache

```
user@host> show security idp ssl-inspection session-id-cache
SSL session identifiers :

c98396c768f983b515d93bb7c421fb6b8ce5c2c5c230b8739b7fcf8ce9c0de4e
a211321a3242233243c3dc0d421fb6b8ce5e4e983b515d932c5c230b87392c

Total SSL session identifiers : 2
```

show security idp status

Syntax show security idp status

Release Information Command introduced in Release 9.2 of Junos OS. Multiple detector information introduced in Release 10.1 of Junos OS.

Description Display the status of the current IDP policy.

Required Privilege Level view

List of Sample Output **show security idp status on page 1476**

Output Fields Table 132 on page 1476 lists the output fields for the **show security idp status** command. Output fields are listed in the approximate order in which they appear.

Table 132: show security idp status Output Fields

Field Name	Field Description
Status of IDP	Status of current IDP policy.
Packets/second	The aggregated throughput (packets per second) for the system.
KBits/second	The aggregated throughput (kbits per second) for the system.
Latency	• min—Minimum delay for a packet to receive and return by a node in microseconds. • max—Maximum delay for a packet to receive and return by a node in microseconds. • ave—Average delay for a packet to receive and return by a node in microseconds.
Packet statistics	Statistics for ICPM, TCP, and UDP packets..

show security idp status

```
user@host> show security idp status
Status of IDP: s0,      Up since: 2009-05-10 08:31:55 UTC (02:07:22 ago)

Packets/second: 0               Peak: 16 @ 2009-05-10 08:35:55 UTC
KBits/second  : 0               Peak: 7 @ 2009-05-10 08:35:55 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 43] [UDP: 0] [Other: 0]
```


Copyright © 2011, Juniper Networks, Inc.

show security idp status detail

Syntax show security idp status detail

Release Information Command introduced in Release 10.1 of Junos OS.

Description Display statistics for each Services Processing Unit (SPU), including multiple detector information on each SPU.

Required Privilege Level view

show security idp status detail

```
user@host> show security idp status detail
  PIC: FPC 0 PIC 0:

  Packets/second: 0             Peak: 16 @ 2009-05-10 08:35:55 UTC
  KBits/second  : 0               Peak: 7 @ 2009-05-10     08:35:55 UTC
  .
  packeet Statistics:

   [ICMP: 0] [TCP: 43] [UDP: 0] [Other: 0]

  Flow Statistics:

   ICMP: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]
   TCP: [Current: 0] [Max: 4 @ 2009-05-10 08:52:58 UTC]
   UDP: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]
   Other: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]

 Status of IDP: PIC : FPC 1 PIC 1:

 Packets/second: 0               Peak: 16 @ 2009-05-10  08:35:55 UTC
 KBits/second  : 0               Peak: 7 @ 2009-05-10 08:35:55 UTC
 Latency (microseconds): [min: 0] [max: 0] [avg: 0]

 Packet Statistics:

  [ICMP: 0] [TCP: 43] [UDP: 0] [Other: 0]

  Flow Statistics:

  ICMP: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]
  TCP: [Current: 0] [Max: 4 @ 2009-05-10 08:52:58 UTC]
  UDP: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]
  Other: [Current: 0] [Max: 0 @ 2009-05-10 08:31:55 UTC]

FPC 0 PIC 0:

  ID   Name   Sessions   Memory   detector
  0    new1     0               10179      9.2.140090324

FPC 1 PIC 1:

 id      name       sessions   memory   detector
 9       idpengine   0         360      9.2.140090340
 8       idpengine   1         360      9.2.140090342
```

show security ike pre-shared-key

Syntax

show security ike pre-shared key
<master-key *master-key* >
<user-id *user-id* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display the Internet Key Exchange (IKE) preshared key used by the Virtual Private network (VPN) gateway to authenticate the remote access user.

Options

master-key ***master-key*** —(Optional) Master preshared key.

user-id ***user-id*** —(Optional) IKE user ID value.

Required Privilege Level

view

Related Documentation

- **pre-shared-key on page 635**

List of Sample Output

show security ike pre-shared-key on page 1478

show security ike pre-shared-key

```
user@host> show security ike pre-shared-key user-id a@juniper.net master-key juniper
Preshared Key:3b33ec3631a561ec5a710f5d02f208033b108bb4
```


Copyright © 2011, Juniper Networks, Inc.

show security ike security-associations

Syntax

show security ike security-associations
<peer-address>
<brief | detail>
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pic *slot-number*>
<family (inet | inet6)>

Release Information

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic**, and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

Description

Display information about Internet Key Exchange security associations (IKE SAs).

Options

none—Display standard information about existing IKE SAs, including index numbers.

peer-address—(Optional) Display details about a particular SA, based on the IPv4 or IPv6 address of the destination peer. This option and **index** provide the same level of output.

brief—(Optional) Display standard information about all existing IKE SAs. (Default)

detail—(Optional) Display detailed information about all existing IKE SAs.

fpc *slot-number*—Specific to SRX Series devices. Display information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.

index *SA-index-number*—(Optional) Display information for a particular SA based on the index number of the SA. To obtain the index number for a particular SA, display the list of existing SAs by using the command with no options. This option and ***peer-address*** provide the same level of output.

kmd-instance —Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- ***kmd-instance-name***—Name of the KMD instance running on the SPU.

pic *slot-number* —Specific to SRX Series devices. Display information about existing IKE SAs in this PIC slot. This option is used to filter the output.

family—(Optional) Display IKE SAs by family. This option is used to filter the output.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

Required Privilege Level

view

Related Documentation

- **clear security ike security-associations on page 1070**

List of Sample Output

show security ike security-associations (IPv4) on page 1482
show security ike security-associations (IPv6) on page 1482
show security ike security-associations detail on page 1482
show security ike security-associations inet6 on page 1483
show security ike security-associations detail (SRX Series Devices) on page 1483
show security ike security-associations index 8 detail on page 1483
show security ike security-associations 1.1.1.2 on page 1484
show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 1484

Output Fields

Table 133 on page 1480 lists the output fields for the **show security ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 133: show security ike security-associations Output Fields

Field Name	Field Description
IKE Peer or Remote Address	IP address of the destination peer with which the local peer communicates.
Index	Index number of an SA. This number is an internally generated number you can use to display information about a single SA.
Location	• **FPC**—Flexible PIC Concentrator (FPC) slot number. • **PIC**—PIC slot number. • **KMD-Instance**—The name of the KMD instance running on the SPU, identified by FPC *slot-number* and PIC *slot-number*. Currently, 4 KMD instances are running on each SPU, and any particular IKE negotiation is carried out by a single KMD instance.
Role	Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.
State	State of the IKE SAs: • **DOWN**—SA has not been negotiated with the peer. • **UP**—SA has been negotiated with the peer.
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.

Copyright © 2011, Juniper Networks, Inc.

Table 133: show security ike security-associations Output Fields *(continued)*

Field Name	Field Description
Mode or Exchange type	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between one another. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are • **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Algorithms	IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:
	• **Authentication**—Type of authentication algorithm used:
	  ◦ **sha1**—Secure Hash Algorithm 1 authentication.
	  ◦ **md5**—MD5 authentication.
	• **Encryption**—Type of encryption algorithm used:
	  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.
	  ◦ **aes-192-cbc**— AES192-bit encryption.
	  ◦ **aes-128-cbc**—AES 128-bit encryption.
	  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.
	  ◦ **des-cbc**—DES encryption.

Traffic statistics	• **Input bytes—**Number of bytes received. • **Output bytes—**Number of bytes transmitted. • **Input packets—**Number of packets received. • **Output packets—**Number of packets transmitted.
Flags	Notification to the key management process of the status of the IKE negotiation: • **caller notification sent**—Caller program notified about the completion of the IKE negotiation. • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.
IPSec security associations	• ***number* created:** The number of SAs created. • ***number* deleted**: The number of SAs deleted.

Copyright © 2011, Juniper Networks, Inc.

Table 133: show security ike security-associations Output Fields *(continued)*

Field Name	Field Description

Phase 2 negotiations in progress	Number of Phase 2 IKE negotiations in progress and status information:
	• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.
	• **Message ID**—Unique identifier for a Phase 2 negotiation.
	• **Local identity**—Identity of the local Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation).
	• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation).
	• **Flags**—Notification to the key management process of the status of the IKE negotiation:
	  ◦ **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  ◦ **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  ◦ **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  ◦ **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.

show security ike security-associations (IPv4)

```
user@host> show security ike security-associations
Index   Remote Address    State  Initiator cookie     Responder cookie     Mode
8  1.1.1.2    UP  3a895f8a9f620198     9040753e66d700bb     Main
Index   Remote Address    State  Initiator cookie     Responder cookie     Mode
9  1.2.1.3     UP  5ba96hfa9f65067   1  70890755b65b80b   d  Main
```

show security ike security-associations (IPv6)

```
user@host> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address

5       UP     e48efd6a444853cf  0d09c59aafb720be  Aggressive     1212::1112
```

show security ike security-associations detail

```
user@host> show security ike security-associations detail
IKE peer 1.1.1.2, Index 8,
 Role: Responder, State: UP
 Initiator cookie: 3a895f8a9f620198, Responder cookie: 9040753e66d700bb
 Exchange type: Main, Authentication method: Pre-shared keys
 Local: 1.1.1.1: 500, Remote: 1.1.1.2:500
 Lifetime: Expired in 381 seconds
 Algorithms:
  Authentication :      md5
  Encryption:         3des-cbc
  Pseudo random function      hmac-md5
 Traffic statistics:
  Input bytes:      11268
  Output bytes:       6940
  Input packets:      57
  Output packets      57
 Flags: Caller notification sent
 IPsec security associations: 0 created, 0 deleted
 Phase 2 negotiations in progress: 1

  Negotiation type: Quick mode, Role: Responder, Message ID: 1765792815
  Local: 1.1.1.1:500, Remote: 1.1.1.2:500
```


Copyright © 2011, Juniper Networks, Inc.

```
  Local identity: No Id
  Remote identity: No Id
  Flags: Caller notification sent, Waiting for remove
```

show security ike security-associations inet6

```
user@host> show security ike security-associations family inet6
  IKE peer 1212::1112, Index 5,
  Role: Initiator, State: UP
  Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aafb720be
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 1212::1111:500, Remote: 1212::1112:500
  Lifetime: Expires in 19518 seconds
  Peer ike-id: not valid
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 1568
   Output bytes  :                 2748
   Input  packets:                    6
   Output packets:                   23
  Flags: Caller notification sent
  IPSec security associations: 5 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Initiator, Message ID: 2900338624
    Local: 1212::1111:500, Remote: 1212::1112:500
    Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Flags: Caller notification sent, Waiting for done
```

show security ike security-associations detail (SRX Series Devices)

```
user@host> show security ike security-associations detail
IKE peer 30.0.0.2, Index 1,
  Location: FPC 1, PIC 2, KMD-Instance 3
  Role: Initiator, State: UP
  Initiator cookie: 58196469ec2df068, Responder cookie: e4de44f4ef333df9
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 20.0.0.4:500, Remote: 30.0.0.2:500
  Lifetime: Expires in 1171 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                  604
   Output bytes  :                 1472
   Input  packets:                    4
   Output packets:                    8
  Flags: Caller notification sent
  IPsec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

show security ike security-associations index 8 detail

```
user@host> show security ike security-associations index 8 detail
IKE peer 1.1.1.2, Index 8
 Role: Responder, State:UP
 Initiator cookie: 3a895f8a9f620198, Responder cookie: 9040753e66d700bb
 Exchange type; main, Authentication method: Pre-shared-keys
 Local: 1.1.1.1:500, Remote: 1.1.1.2:500
 Lifetime: Expired in 381 seconds
```

```
Algorithms:
 Authentication:       md5
 Encryption:      3des-cbc
 Pseudo random function      hmac-md5
Traffic statistics:
 Input bytes:       11268
 Output bytes:        6940
 Input packets:        57
 Output packets:        57
Flags: Caller notification sent
IPsec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

 Negotiation type: Quick mode, Role: Responder, Message ID: 1765792815
 Local: 1.1.1.1:500, Remote: 1.1.1.2:500
 Local identity: No Id
 Remote identity: No Id
 Flags: Caller notification sent, Waiting for remove
```

show security ike security-associations 1.1.1.2

```
user@host> show security ike security-associations 1.1.1.2
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode

8       1.1.1.2         UP     3a895f8a9f620198  9040753e66d700bb  Main
```

show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```
user@host> show security ike security-associations fpc 6 pic 1 kmd-instance all
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode

1728053250 1.1.1.2      UP     fc959afd1070d10b  bdeb7e8c1ea99483  Main
```


Copyright © 2011, Juniper Networks, Inc.

show security ipsec next-hop-tunnels

Syntax

show security ipsec next-hop-tunnels
< interface-name ***interface-name*** **>**

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display security information about the secure tunnel interface.

Options

none—Display information about all secure tunnel interface.

interface-name ***interface-name*** —(Optional) Name of the secure tunnel logical interface.

Required Privilege Level

view

List of Sample Output

show security ipsec next-hop-tunnels on page 1485

Output Fields

Table 134 on page 1485 lists the output fields for the **show security ipsec next-hop-tunnels** command. Output fields are listed in the approximate order in which they appear.

Table 134: show security ipsec next-hop-tunnels Output Fields

Field Name	Field Description
Next-hop gateway	IP address of the next gateway.
Interface	Name of the secure tunnel logical interface.
IPsec VPN name	Name of the IPsec VPN tunnel.
Flag	• **Static**—IP address manually configured. • **Auto**—IP address obtained from the remote peer automatically.

show security ipsec next-hop-tunnels

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface   IPsec VPN name                    Flag
11.1.1.2          st0.0       autokey                           Static
11.1.1.3          st0.0       pbd-4-6                           Auto
```

show security ipsec security-associations

Syntax

show security ipsec security-associations
<brief | detail>
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pic *slot-number*>
<family (inet | inet6)>

Release Information

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic**, and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

Description

Display information about the IPsec security associations (SAs).

Options

none—Display information about all SAs.

brief | **detail**—(Optional) Display the specified level of output.

fpc ***slot-number***—Specific to SRX Series devices. Display information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.

index ***SA-index-number***—(Optional) Display detailed information about the specified SA identified by this index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

kmd-instance—Specific to SRX Series devices. Display information about existing IPsec SAs in the key management process (the daemon, which in this case is KMD) identified by the FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- ***kmd-instance-name***—Name of the KMD instance running on the SPU.

pic ***slot-number***—Specific to SRX Series devices. Display information about existing IPsec SAs in this PIC slot. This option is used to filter the output.

family—(Optional) Display SAs by family. This option is used to filter the output.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

Required Privilege Level

view

Related Documentation

- **clear security ipsec security-associations on page 1072**

List of Sample Output

show security ipsec security-associations (IPv4) on page 1489
show security ipsec security-associations (IPv6) on page 1489
show security ipsec security-associations index on page 1490
show security ipsec security-associations brief on page 1490

Copyright © 2011, Juniper Networks, Inc.

show security ipsec security-associations detail on page 1490
show security ipsec security-associations detail (SRX Series Devices) on page 1491
show security ipsec security-associations inet6 on page 1491
show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 1491

Output Fields Table 135 on page 1487 lists the output fields for the **show security ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 135: show security ipsec security-associations

Field Name	Field Description
Total active tunnels	Total number of active IPsec tunnels.
ID	Index number of the SA. You can use this number to get additional information about the SA.
Gateway	IP address of the remote gateway.
Port	If Network Address Translation (NAT) is used, this value is 4500. Otherwise it is the standard IKE port, 500.
Algorithm	Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes • An authentication algorithm used to authenticate exchanges between the peers. Options are **hmac-md5-95**, **hmac-sha1-96, or ESP.** • An encryption algorithm used to encrypt data traffic. Options are **3des-cbc, aes-128-cbc, aes-192-cbc**, **aes-256-cbc**, or **des-cbc.**
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.
Life: sec/kb	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.
Sta	State has two options, Installed and Not Installed. • Installed—The SA is installed in the SA database. • Not Installed—The SA is not installed in the SA database. For transport mode, the value of State is always Installed.
Mon	The Mon field refers to VPN monitoring status. If VPN monitoring is enabled, then thisfield displays **U** (up) or **D** (down). A hyphen (-) means VPN monitoring is not enabled for this SA.
vsys or Virtual-system	The root system.
Tunnel index	Numeric identifier of the specific IPsec tunnel for the SA.
Local gateway	Gateway address of the local system.

Copyright © 2011, Juniper Networks, Inc.

Table 135: show security ipsec security-associations *(continued)*

Field Name	Field Description
Remote gateway	Gateway address of the remote system.
Local identity	Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN).
Remote identity	IP address of the destination peer gateway.
DF-bit	State of the don't fragment bit: set or cleared.
Policy-name	Name of the applicable policy.
Location	**FPC**—Flexible PIC Concentrator (FPC) slot number. **PIC**—PIC slot number. **KMD-Instance**—The name of the KMD instance running on the SPU, identified by FPC *slot-number* and PIC *slot-number*. Currently, 4 KMD instances running on each SPU, and any particular IPsec negotiation is carried out by a single KMD instance.
Direction	Direction of the SA; it can be inbound or outbound.
AUX-SPI	Value of the auxiliary security parameter index(SPI). • When the value is **AH** or **ESP**, **AUX-SPI** is always 0. • When the value is **AH+ESP**, **AUX-SPI** is always a positive integer.
Mode	Mode of the SA: • **transport**—Protects host-to-host connections. • **tunnel**—Protects connections between security gateways.
Type	Type of the SA: • **manual**—Security parameters require no negotiation. They are static and are configured by the user. • **dynamic**—Security parameters are negotiated by the IKE protocol. Dynamic SAs are not supported in transport mode.
State	State of the SA: • **Installed**—The SA is installed in the SA database. • **Not Installed**—The SA is not installed in the SA database. For transport mode, the value of State is always Installed.

Copyright © 2011, Juniper Networks, Inc.

Table 135: show security ipsec security-associations *(continued)*

Field Name	Field Description

Protocol	Protocol supported.
	• Transport mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH).
	• Tunnel mode supports ESP and AH.
	  ◦ **Authentication**—Type of authentication used.
	  ◦ **Encryption**—Type of encryption used.

Soft lifetime	The soft lifetime informs the IPsec key management system that the SA is about to expire. Each lifetime of a SA has two display options, hard and soft, one of which must be present for a dynamic SA. This allows the key management system to negotiate a new SA before the hard lifetime expires. • **Expires in seconds**—Number of seconds left until the SA expires.
Hard lifetime	The hard lifetime specifies the lifetime of the SA. • **Expires in seconds**—Number of seconds left until the SA expires.
Lifesize Remaining	The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited. • **Expires in kilobytes**—Number of kilobytes left until the SA expires.
Anti-replay service	State of the service that prevents packets from being replayed. It can be **Enabled** or **Disabled**.
Replay window size	Configured size of the antireplay service window. It can be 32 or 64 packets. If the replay window size is 0, the antireplay service is disabled. The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets.

show security ipsec security-associations (IPv4)

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys
  131075 11.0.28.241    500   ESP:3des/sha1   86758ff0 6918/ unlim   -   0
  131075 11.0.28.241    500   ESP:3des/sha1   3183ff26 6918/ unlim   -   0
```

show security ipsec security-associations (IPv6)

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID    Algorithm       SPI      Life:sec/kb  Mon vsys Port  Gateway
  131074 ESP:3des/sha1 14caf1d9 3597/ unlim   -   root 500   1212::1112
  131074 ESP:3des/sha1 9a4db486 3597/ unlim   -   root 500   1212::1112
```

show security ipsec security-associations index

```
user@host> show security ipsec security-associations index 5
Virtual-system: Root
Local gateway: 1.1.1.1, Remote gateway: 1.1.1.2
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0...7]=0.0.0.0/0)
DF-bit: clear
Policy-name: my-policy

Direction: inbound, SPI: 494001027, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expired
Hard lifetime: Expired in 130 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: inbound, SPI: 1498711950, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound, SPI: 4038397695, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64
```

show security ipsec security-associations brief

```
user@host> show security ipsec security-associations brief
Total active tunnels: 2
ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys
<16384 1.1.1.1 500 ESP:3des/sha1 af88baa 28795/unlim D 0
>16384 1.1.1.1 500 ESP:3des/sha1 f4e3e5f4 28795/unlim D 0
```

show security ipsec security-associations detail

```
user@host> show security ipsec security-associations detail
Virtual-system: Root
Local Gateway: 1.1.1.2, Remote Gateway: 1.1.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
DF-bit: clear

Direction: inbound, SPI: 184060842, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32

Direction: outbound, SPI: 4108576244, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32
```


Copyright © 2011, Juniper Networks, Inc.

show security ipsec security-associations detail (SRX Series Devices)

```
user@host> show security ipsec security-associations detail
  Virtual-system: Root
  Local Gateway: 20.0.0.4, Remote Gateway: 30.0.0.2
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4(any:0,[0..3]=20.0.0.4)
    DF-bit: clear
    Policy-name: p1

    Location: FPC 1, PIC 2, KMD-Instance 3
    Direction: inbound, SPI: 3727011331, AUX-SPI: 0
    Hard lifetime: Expires in 3570 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 3525 seconds
    Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: enabled, Replay window size: 32

    Location: FPC 1, PIC 2, KMD-Instance 3
    Direction: outbound, SPI: 4212479378, AUX-SPI: 0
    Hard lifetime: Expires in 3570 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 3525 seconds
    Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: enabled, Replay window size: 32
```

show security ipsec security-associations inet6

```
user@host> show security ipsec security-associations family inet6
  Virtual-system: root
  Local Gateway: 1212::1111, Remote Gateway: 1212::1112
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Direction: inbound, SPI: 14caf1d9, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3440 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2813 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: 9a4db486, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3440 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2813 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
```

show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```
user@host> show security ipsec security-associations fpc 6 pic 1 kmd-instance all
  Total active tunnels: 1

ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys

<2    1.1.1.2          500   ESP:3des/sha1   67a7d25d 28280/unlim   -   0

>2    1.1.1.2          500   ESP:3des/sha1   a23cbcdc 28280/unlim   -   0
```

show security ipsec statistics

Syntax

show security ipsec statistics
<**fpc** *slot-number* >
<**index** *SA-index-number* >
<**kmd-instance** *kmd-instance-name* >
pic *slot-number*

Release Information

Command introduced in Release 8.5 of Junos OS; **fpc** and **pic** options added in Release 9.3 of Junos OS ;**kmd-instance** option added in Release 10.4 of Junos OS.

Description

Display standard IPsec statistics.

Options

none—Display statistics about all IPsec security associations (SAs).

fpc ***slot-number*** —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.

index ***SA-index-number*** —(Optional) Display statistics for the SA with this index number.

kmd-instance ***kmd-instance-name*** —Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.

- **all**—All KMD instances running on the Services Processing Unit (SPU).
- ***kmd-instance-name***—Name of the KMD instance running on the SPU.

pic ***slot-number*** —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this PIC slot. This option is used to filter the output.

Required Privilege Level

view

Related Documentation

- **clear security ipsec statistics on page 1074**

List of Sample Output

show security ipsec statistics on page 1493
show security ipsec statistics index 5 on page 1493
show security ipsec statistics fpc 6 pic 1 (SRX Series devices) on page 1494

Output Fields

Table 136 on page 1492 lists the output fields for the **show security ipsec statistics** command. Output fields are listed in the approximate order in which they appear.

Table 136: show security ipsec statistics Output Fields

Field Name	Field Description
Virtual-system	The root system.

Copyright © 2011, Juniper Networks, Inc.

Table 136: show security ipsec statistics Output Fields *(continued)*

Field Name	Field Description
ESP Statistics	• **Encrypted bytes**—Total number of bytes encrypted by the local system across the IPsec tunnel. • **Decrypted bytes**—Total number of bytes decrypted by the local system across the IPsec tunnel. • **Encrypted packets**—Total number of packets encrypted by the local system across the IPsec tunnel. • **Decrypted packets**—Total number of packets decrypted by the local system across the IPsec tunnel.
AH Statistics	• **Input bytes**—Total number of bytes received by the local system across the IPsec tunnel. • **Output bytes**—Total number of bytes transmitted by the local system across the IPsec tunnel. • **Input packets**—Total number of packets received by the local system across the IPsec tunnel. • **Output packets**—Total number of packets transmitted by the local system across the IPsec tunnel.
Errors	• **AH authentication failures**—Total number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel. • **Replay errors**—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window. • **ESP authentication failures**—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets. • **ESP decryption failures**—total number of ESP decryption errors. • **Bad headers**—Total number of invalid headers detected. • **Bad trailers**—Total number of invalid trailers detected.

show security ipsec statistics

```
user@host> show security ipsec statistics
Virtual-system: Root
ESP Statistics:
  Encrypted bytes:                0
  Decrypted bytes:                0
  Encrypted packets:              0
  Decrypted packets:              0
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

show security ipsec statistics index 5

```
user@host> show security ipsec statistics index 5
Virtual-system: Root
SA index: 5
ESP Statistics:
```

```
  Encrypted bytes:                0
  Decrypted bytes:                0
  Encrypted packets:              0
  Decrypted packets:              0
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

show security ipsec statistics fpc 6 pic 1 (SRX Series devices)

```
user@host> show security ipsec statistics fpc 6 pic 1
ESP Statistics:
Encrypted bytes:           536408
Decrypted bytes:           696696
Encrypted packets:           1246
Decrypted packets:            888
AH Statistics:
Input bytes:                    0
Output bytes:                   0
Input packets:                  0
Output packets:                 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```


Copyright © 2011, Juniper Networks, Inc.

show security match-policies

Syntax

show security match-policies
from-zone *zone-name*
to-zone *zone-name*
source-ip *ip-address*
destination-ip *ip-address*
source-port *port-number*
destination-port *port-number*
protocol *protocol-name* | *protocol-number*
result-count *number*

Release Information

Command introduced in Release 10.3 of Junos OS.
Command updated in Release 10.4 of Junos OS.

Description

The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, then the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are "shadowed" by the first and are never encountered by matching traffic.

NOTE: The **show security match-policies** command is applicable only to security policies; IDP policies are not supported.

Options

from-zone ***from-zone***—Name or ID of the source zone of the traffic.

to-zone ***to-zone***—Name or ID of the destination zone of the traffic.

source-ip ***source-ip***—Source IP address of the traffic

destination-ip ***destination-ip***—Destination IP address of the traffic.

source-port ***source-port***—Source port number of the traffic. Range is 1 through 65,535.

destination-port ***destination-port***—Destination port number of the traffic. Range is 1 through 65,535

protocol ***protocol-name*** | ***protocol-number***—Protocol name or numeric value of the traffic.

- **ah** or **51**
- **egp** or **8**
- **esp** or **50**

Copyright © 2011, Juniper Networks, Inc.

- **gre** or **47**
- **icmp** or **1**
- **igmp** or **2**
- **igp** or **9**
- **ipip** or **94**
- **ipv6** or **41**
- **ospf** or **89**
- **pgm** or **113**
- **pim** or **103**
- **rdp** or **27**
- **rsvp** or **46**
- **sctp** or **132**
- **tcp** or **6**
- **udp** or **17**
- **vrrp** or **112**

result-count *number*—(Optional) The number of policy matches to display. Valid range is from 1 through 16. The default value is 1.

Required Privilege Level view

Related Documentation

- **clear security policies statistics on page 1079**

List of Sample Output

Example 1: show security match-policies on page 1498
Example 2: show security match policies ... result-count on page 1498

Output Fields Table 137 on page 1496 lists the output fields for the **show security match-policies** command. Output fields are listed in the approximate order in which they appear.

Table 137: show security match-policies Output Fields

Field Name	Field Description
Policy:	Name of the applicable policy.

Copyright © 2011, Juniper Networks, Inc.

Table 137: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Action or **Action-type:**	The action to be taken for traffic that matches the policy's match criteria. Actions include the following: • **permit** • **firewall-authentication** • **tunnel ipsec-vpn** *vpn-name* • **pair-policy** *pair-policy-name* • **source-nat pool** *pool-name* • **pool-set** *pool-set-name* • **interface** • **destination-nat** *name* • **deny** • **reject**
State:	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index:	An internal number associated with the policy.
Sequence number:	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.
From zone:	Name of the source zone.
To zone:	Name of the destination zone.
Source addresses:	The names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses:	The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it.
Application	Name of a preconfigured or custom application, or **any** if no application is specified.
IP protocol:	Numeric value for the IP protocol used by the application, such as 6 for TCP or 1 for ICMP.
ALG:	If an ALG is associated with the session, the name of the ALG. Otherwise, 0.
Inactivity timeout:	Elapsed time without activity after which the application is terminated.
Source-port range:	Range of matching source ports defined in the policy.

Copyright © 2011, Juniper Networks, Inc.

Table 137: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Destination-port range:	Range of matching destination ports defined in the policy.

Example 1: show security match-policies

```
user@host> show security match-policies from-zone z1 to-zone z2 source-ip 10.10.10.1
destination-ip 30.30.30.1 source-port 1 destination-port 21 protocol tcp
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 20.20.0.0/16
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 40.40.0.0/16
    d3: 30.30.30.1/32
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [21-21]
```

Example 2: show security match policies ... result-count

```
user@host> show security match-policies source-ip 10.10.10.1 destination-ip 20.20.20.5
source_port 1004 destination_port 80 protocol tcp result_count 5
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 20.20.0.0/16
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
    Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
  Sequence number: 15
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa11: 10.10.10.1/32
  Destination addresses:
    da15: 20.20.20.5/32
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
    Source port range: [1000-1030]
    Destination port range: [80-80]
```


Copyright © 2011, Juniper Networks, Inc.

show security monitoring fpc fpc-number

Syntax

show security monitoring fpc *fpc-number*
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 9.2 of Junos OS.

Description

Display security monitoring information about the FPC slot.

Options

fpc-number —Display security monitoring information for the specified FPC slot. It can be in the range from 0 to 11.

node—(Optional) For chassis cluster configurations, display security monitoring information for the specified FPC on a specific node (device) in the cluster.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security monitoring fpc 0 on page 1500
show security monitoring fpc 1 on page 1500
show security monitoring fpc 8 on page 1500

Output Fields

Table 138 on page 1499 lists the output fields for the **show security monitoring fpc** *fpc-number* command. Output fields are listed in the approximate order in which they appear.

Table 138: show security monitoring fpc fpc-number Output Fields

Field Name	Field Description
FPC	Slot number in which the FPC is installed.
PIC	Slot number in which the PIC is installed.
CPU Utilization (%)	Total percentage of CPU being used by the PIC's processors.
Memory Utilization (%)	Percentage of heap space (dynamic memory) being used by the PIC's processor. If this number exceeds 80 percent, there may be a software problem (memory leak).
Current flow session	The current number of flow sessions. When SRX Series devices operate in packet mode, flow sessions will not be created and this field will remain zero.
Max flow session	The maximum number of flow sessions allowed. This number will differ from one device to another.

Copyright © 2011, Juniper Networks, Inc.

Table 138: show security monitoring fpc fpc-number Output Fields *(continued)*

Field Name	Field Description
SPU current cp session	The current number of cp sessions for the SPU (on SRX3400, SRX3600, SRX5600, and SRX5800 devices only).
SPU max cp session	The maximum number of cp sessions allowed for the SPU (on SRX3400, SRX3600, SRX5600, and SRX5800 devices only).

show security monitoring fpc 0

```
user@host> show security monitoring fpc 0
FPC 0
  PIC 0
    CPU utilization   :    0 %
    Memory Utilization:   65 %
    Current flow session :   0
    Max flow session  : 131072
```

show security monitoring fpc 1

```
user@host> show security monitoring fpc 1
FPC 1
  PIC 0
    CPU utilization   :    0 %
    Memory Utilization:   67 %
  PIC 1
    CPU utilization   :    0 %
    Memory Utilization:   67 %
```

show security monitoring fpc 8

```
user@host> show security monitoring fpc 8
node0:
--------------------------------------------------------------------------
FPC 8
  PIC 0
    CPU utilization   :    0 %
    Memory Utilization:   74 %
node1:
--------------------------------------------------------------------------
FPC 8
  PIC 0
    CPU utilization   :    0 %
    Memory Utilization:   74 %
  PIC 1
    CPU utilization   :    0 %
    Memory Utilization:   43 %
```


Copyright © 2011, Juniper Networks, Inc.

show security monitoring performance session

Syntax

show security monitoring performance session

```
<fpc slot-number>

<pic slot-number>
```

Release Information

Command introduced in Release of 10.2 of Junos OS.

Description

Display the number of sessions added (ramp-up rate) for the last 60 seconds. Output of this command does not display the total number of sessions or the number of deleted sessions.

Options

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.

NOTE: The fpc slot-number and pic slot-number options are not available on SRX100, SRX210, SRX240, and SRX650 devices.

Required Privilege Level

View

show security monitoring performance session

user@host> show security monitoring performance session

```
fpc  0  pic  0
Last 60 seconds:
 0:       8   1:       8   2:       8   3:       8   4:       8   5:       7
 6:       7   7:       7   8:       7   9:       7  10:       7  11:       8
12:       8  13:       8  14:       7  15:       7  16:       7  17:       7
18:       7  19:       7  20:       7  21:       5  22:       5  23:       5
24:       5  25:       5  26:       5  27:       5  28:       5  29:       4
30:       4  31:       4  32:       3  33:       3  34:       3  35:       3
36:       5  37:       5  38:       6  39:       6  40:       5  41:       5
42:       5  43:       5  44:       5  45:       5  46:       5  47:       5
48:       7  49:       7  50:       6  51:       8  52:       8  53:       6
54:       5  55:       7  56:       7  57:       5  58:       5  59:       8
```

show security monitoring performance spu

Syntax

show security monitoring performance spu

```
<fpc slot-number>

<pic slot-number>
```

Release Information

Command introduced in Release 10.2 of Junos OS.

Description

Display the services processing unit (SPU) statistics for all FPC slots over the last 60 seconds.

Options

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.

NOTE: The fpc slot-number and pic slot-number options are not available on SRX100, SRX210, SRX240, and SRX650 devices.

Required Privilege Level

View

show security monitoring performance spu

user@host>show security monitoring performance spu

```
fpc  0  pic  0
Last 60 seconds:
 0:  48   1:  48   2:  48   3:  48   4:  48   5:  48
 6:  48   7:  48   8:  49   9:  48  10:  48  11:  48
12:  48  13:  48  14:  48  15:  48  16:  48  17:  48
18:  48  19:  48  20:  48  21:  48  22:  49  23:  48
24:  49  25:  49  26:  48  27:  48  28:  48  29:  48
30:  48  31:  48  32:  48  33:  48  34:  48  35:  48
36:  46  37:  47  38:  46  39:  46  40:  46  41:  46
42:  46  43:  46  44:  46  45:  46  46:  46  47:  46
48:  46  49:  46  50:  46  51:  46  52:  46  53:  46
54:  46  55:  46  56:  46  57:  46  58:  46  59:  46
```


Copyright © 2011, Juniper Networks, Inc.

show security nat destination pool

Syntax

show security nat destination pool
< *pool-name* >
all

Release Information

Command introduced in Release 9.2 of Junos OS.

Description

Display information about the specified Network Address Translation (NAT) destination address pool.

Options

pool-name —Name of the destination address pool.

all—Display information about all the destination NAT address pool.

Required Privilege Level

view

Related Documentation

- **pool (Destination NAT) on page 626**

List of Sample Output

show security nat destination pool dst-nat-pool1 on page 1503
show security nat destination pool all on page 1504

Output Fields

Table 139 on page 1503 lists the output fields for the **show security nat destination pool** command. Output fields are listed in the approximate order in which they appear.

Table 139: show security nat destination pool Output Fields

Field Name	Field Description
Pool Name	Name of the destination pool.
Pool id	Pool identification number.
Routing Instance	Name of the routing instance.
Total address	Number of IP addresses that are in use.
Address available	Number of IP addresses that are free for use.
Address range	IP address or IP address range for the pool.
Port	Port number.
Total destination nat pool number	Number of destination NAT pools.

show security nat destination pool dst-nat-pool1

```
user@host> show security nat destination pool dst-nat-pool1
    Pool name:         dst-nat-pool1
    Pool id:           1
    Routing instance:  ri-green
```

```
    Total address:     1
    Address available: 1
    Address range                   Port
    10.1.1.150-10.1.1.150
```

show security nat destination pool all

```
user@host> show security nat destination pool all
    Total destination nat pool number: 3

    Pool name:         dst-nat-pool1
    Pool id:           1
    Routing instance:  ri-green
    Total address:     1
    Address available: 1
    Address range                   Port
    10.1.1.150-10.1.1.150
    Pool name:         dst-nat-pool2
    Pool id:           2
    Routing instance:  ri-green
    Total address:     21
    Address available: 10
    Address range                   Port
    10.1.1.160-10.1.1.180
    Pool name:         dst-nat-pool3
    Pool id:           3
    Routing instance:  ri-green
    Total address:     1
    Address available: 1
    Address range                   Port
    10.1.1.190-10.1.1.190           8080
```


Copyright © 2011, Juniper Networks, Inc.

show security nat destination rule

Syntax

show security nat destination rule
<rule-name>
all

Release Information

Command introduced in Release 9.2 of Junos OS.

Description

Display information about the specified destination Network Address Translation (NAT) rule.

Options

rule-name—Name of the rule.

all—Display information about all the destination NAT rule.

Required Privilege Level

view

Related Documentation

- **rule (Destination NAT) on page 681**

List of Sample Output

show security nat destination rule r4 on page 1506
show security nat destination rule all on page 1506

Output Fields

Table 140 on page 1505 lists the output fields for the show security nat destination rule command. Output fields are listed in the approximate order in which they appear.

Table 140: show security nat destination rule Output Fields

Field Name	Field Description
Destination nat rule	Name of the destination NAT rule.
State	Status of the IP address: • **Active**—Denotes that the IP address is in use. • **Free**—IP address is available for allocation.
Index	Rule index number.
From routing instance	Name of the routing instance from which the packet comes.
Source address	Name of the source addresses which match the rule. The default value is any.
Destination address	Name of the destination addresses which match the rule. The default value is any.
Destination ports	Destination ports number which match the rule. The default value is any.

Copyright © 2011, Juniper Networks, Inc.

Table 140: show security nat destination rule Output Fields *(continued)*

Field Name	Field Description
Action	The action taken in regard to a packet that matches the rule's tuples. Actions include the following: • **destination-nat**—Use user-defined destination NAT pool to perform destination NAT. • **ui**—Do not perform destination NAT.
Hit times	Number of times a translation in the translation table is used for a destination NAT rule.
Fail times	Number of times a translation in the translation table failed to translate for a destination NAT rule.
Total destination nat rule number	Number of destination NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the destination NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the destination NAT rules.

show security nat destination rule r4

```
user@host>show security nat destination rule r4
Destination nat rule: r4, State: enabled, Index: 7
      From routing instance: ri-1
      Source addresses:
        any: 0.0.0.0/0
      Destination addresses:
        1.1.1.1/32 1.1.1.3/32
      Destination ports:
        any: 0
      Action: destination-nat pool d1

      Hit times: 30
      Fail times: 0
```

show security nat destination rule all

```
user@host>  show security nat destination rule all

Total destination nat rule number: 2
    Total hit times: 45
    Total fail times: 3

    Destination nat rule: r4, State: enabled, Index: 7
      From routing instance: ri-1
      Source addresses:
        any: 0.0.0.0/0
      Destination addresses:
        1.1.1.1/32 1.1.1.3/32
      Destination ports:
        any: 0
      Action: destination-nat pool d1

      Hit times: 30
      Fail times: 0

    Destination nat rule: r5, State: enabled, Index: 8
```


Copyright © 2011, Juniper Networks, Inc.

```
From routing instance: ri-1, interface: fe-0/0/0.0
Source addresses:
  any: 0.0.0.0/0
Destination addresses:
  1.1.1.1/32
Destination ports:
  any: 0
Action: destination-nat pool d3

Hit times: 15
Fail times: 3
```

show security nat destination summary

Syntax show security nat destination summary

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display a summary of Network Address Translation (NAT) destination pool information.

Required Privilege Level view

Related Documentation
- **pool (Destination NAT) on page 626**
- **rule (Destination NAT) on page 681**

List of Sample Output **show security nat destination summary on page 1508**

Output Fields Table 141 on page 1508 lists the output fields for the **show security nat destination summary** command. Output fields are listed in the approximate order in which they appear.

Table 141: show security nat destination summary Output Fields

Field Name	Field Description
Total destination nat pool number	Number of destination NAT pools.
Pool name	Name of the destination address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
Port	Port number.
Total	Number of IP addresses that are in use.
Available	Number of IP addresses that are free for use.
Total destination nat rule number	Number of destination NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the destination NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the destination NAT rules.

show security nat destination summary

```
user@host> show security nat destination summary
    Total destination nat pool number: 3
    Pool name            Address range    Routing instance  Port Total Available

    dst-nat-pool1     10.1.1.150-10.1.1.150    ri-green            1     1
```

 Copyright © 2011, Juniper Networks, Inc.

```
dst-nat-pool2     10.1.1.160-10.1.1.180    ri-green            21    10
dst-nat-pool3     10.1.1.190-10.1.1.190    ri-green     8080   1     1

Total destination nat rule number: 2
Total hit times: 45
Total fail times: 3
```

show security nat incoming-table

Syntax

show security nat incoming-table
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display Network Address Translation (NAT) table information.

Options

none—Display all information NAT incoming table.

node—(Optional) For chassis cluster configurations, display incoming table information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **clear security nat incoming-table on page 1075**

List of Sample Output

show security nat incoming-table on page 1511

Output Fields

Table 142 on page 1510 lists the output fields for the **show security nat incoming-table** command. Output fields are listed in the approximate order in which they appear.

Table 142: show security nat incoming-table Output Fields

Field Name	Field Description
In use	Number of entries in the NAT table.
Maximum	Maximum number of entries possible in the NAT table.
Entry allocation failed	Number of entries failed for allocation.
Destination	Destination IP address and port number.
Host	Host IP address and port number that the destination IP address is mapped.
References	Number of sessions referencing the entry.
Timeout	Timeout, in seconds, of the entry in the NAT table.
Source-pool	Name of source pool where translation is allocated.

Copyright © 2011, Juniper Networks, Inc.

show security nat incoming-table

```
user@host> show security nat incoming-table
In use: 1, Maximum: 1024, Entry allocation failed: 0
Destination           Host                  References Timeout Source-pool
10.1.1.26:1028        1.1.1.10:5060                  1    3600 p1
```

show security nat interface-nat-ports

Syntax

show security nat interface-nat-ports
<node (*node-id* | all | local | primary)>

Release Information

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display port usage for an interface source pool for Network Address Translation (NAT).

Options

none—Display all port usage information for an interface source pool.

node—(Optional) For chassis cluster configurations, display interface NAT ports information on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security nat interface-nat-ports on page 1512

Output Fields

Table 143 on page 1512 lists the output fields for the **show security nat interface-nat-ports** command. Output fields are listed in the approximate order in which they appear.

Table 143: show security nat interface-nat-ports Output Fields

Field Name	Field Description
Pool Index	Port pool index.
Total Ports	Total number of ports in a port pool. In SRX Series devices, 10 interface NAT ports are supported.
Single Ports Allocated	Number of ports allocated one at a time that are in use.
Single Ports Available	Number of ports allocated one at a time that are free for use.
Twin Ports Allocated	Number of ports allocated two at a time that are in use.
Twin Ports Available	Number of ports allocated two at a time that are free for use.

show security nat interface-nat-ports

```
user@host> show security nat interface-nat-ports
Pool   Total  Single ports  Single ports  Twin ports  Twin ports
    index  ports     allocated     available   allocated   available
     0  64510             0         63486           0        1024
     1  64510             0         63486           0        1024
```


Copyright © 2011, Juniper Networks, Inc.

2	64510	0	63486	0	1024
3	64510	0	63486	0	1024
4	64510	0	63486	0	1024
5	64510	0	63486	0	1024
6	64510	0	63486	0	1024
7	64510	0	63486	0	1024
8	64510	0	63486	0	1024
9	64510	0	63486	0	1024

Copyright © 2011, Juniper Networks, Inc.

show security nat source persistent-nat-table

Syntax show security nat source persistent-nat-table (all | interface | internal-ip *ip-address* <internal-port *port*> | pool *poolname*)

Release Information Command introduced in Release 9.6 of Junos OS.

Description Display a summary of persistent Network Address Translation (NAT) information.

Options **all**—Display all persistent NAT bindings.

interface—Display persistent NAT bindings for the interface.

internal-ip ***ip-address***—Display persistent NAT bindings for the specified internal IP address.

internal-ip ***ip-address*** **internal-port** ***port***—Display persistent NAT bindings for the specified internal IP address and port.

pool—Display persistent NAT bindings for the specified source NAT pool.

Required Privilege Level view

Related Documentation

- **clear security nat source persistent-nat-table on page 1076**

List of Sample Output

show security nat source persistent–nat–table all on page 1515
show security nat source persistent–nat–table internal-ip 10.10.10.197 on page 1515
show security nat source persistent–nat–table internal-ip 10.10.10.197 internal-port 6000 on page 1515
show security nat source persistent–nat–table interface on page 1515

Output Fields Table 144 on page 1514 lists the output fields for the **show security nat source persistent–nat–table** command. Output fields are listed in the approximate order in which they appear.

Table 144: show security nat source persistent–nat–table Output Fields

Field Name	Field Description
Internal IP/Port	Internal transport IP address and port number of the outgoing session from internal to external.
Reflexive IP/Port	Translated IP address and port number of the source IP address and port.
Source NAT Pool	The name of the source pool where persistent NAT is used.
Type	Persistent NAT type.
Left_time/Conf_time	The inactivity timeout period that remains and the configured timeout value.
Current_Sess_Num/Max_Sess_Num	The number of current sessions associated with the persistent NAT binding.

 Copyright © 2011, Juniper Networks, Inc.

Table 144: show security nat source persistent–nat–table Output Fields *(continued)*

Field Name	Field Description
Source NAT Rule	Name of the source NAT rule to which this persistent NAT binding applies.

show security nat source persistent–nat–table all

```
user@host> show security nat source persistent–nat–table all
Persistent NAT Table Statistics:
  binding total    : 131072
  binding in use   : 1
  enode total      : 1048576
  enode in use     : 0
     Internal                Reflective          Source     Type
Left_time/  Curr_Sess_Num/  Source
 In_IP          In_Port Ref_IP          Ref_Port NAT Pool
Conf_time   Max_Sess_Num    NAT Rule

10.10.10.197    6000    200.200.200.241 6000     src-nat-by-shifting
any-remote-host    -/300   1/30     cone_nat
```

show security nat source persistent–nat–table internal-ip 10.10.10.197

```
user@host> show security nat source persistent–nat–table internal-ip 10.10.10.197
Persistent NAT Table Statistics:
  binding total    : 131072
  binding in use   : 1
  enode total      : 1048576
  enode in use     : 0
     Internal                Reflective          Source     Type
Left_time/  Curr_Sess_Num/  Source
 In_IP          In_Port Ref_IP          Ref_Port NAT Pool
Conf_time   Max_Sess_Num    NAT Rule

10.10.10.197    6000    200.200.200.241 6000     src-nat-by-shifting
any-remote-host    -/300   1/30     cone_nat
```

show security nat source persistent–nat–table internal-ip 10.10.10.197 internal-port 6000

```
user@host> show security nat source persistent–nat–table internal-ip 10.10.10.197 internal-port
6000
Persistent NAT Table Statistics:
  binding total    : 131072
  binding in use   : 1
  enode total      : 1048576
  enode in use     : 0
     Internal                Reflective          Source     Type
Left_time/  Curr_Sess_Num/  Source
 In_IP          In_Port Ref_IP          Ref_Port NAT Pool
Conf_time   Max_Sess_Num    NAT Rule

10.10.10.197    6000    200.200.200.241 6000     src-nat-by-shifting
any-remote-host    -/300   1/30     cone_nat
```

show security nat source persistent–nat–table interface

```
user@host> show security nat source persistent–nat–table interface
Persistent NAT Table Statistics:
  binding total    : 131072
  binding in use   : 1
  enode total      : 1048576
```

```
                    enode in use     : 0
```


Copyright © 2011, Juniper Networks, Inc.

show security nat source pool

Syntax

show security nat source pool
< *pool-name* >
all

Release Information

Command introduced in Release 9.2 of Junos OS.

Description

Display information about the specified Network Address Translation (NAT) source address pool.

Options

pool-name —Name of the source pool.

all—Display information about all the source NAT address pool.

Required Privilege Level

view

Related Documentation

- **pool (Source NAT) on page 626**

List of Sample Output

show security nat source pool src-nat-pool1 on page 1518
show security nat source pool all on page 1518

Output Fields

Table 145 on page 1517 lists the output fields for the **show security nat source pool** command. Output fields are listed in the approximate order in which they appear.

Table 145: show security nat source pool Output Fields

Field Name	Field Description
Pool name	Name of the source pool.
Pool id	Pool identification number.
Routing Instance	Name of the routing instance.
Port range	Port number range for the pool.
Total address	Number of IP addresses that are in use.
Address available	Number of IP addresses that are free for use.
Address range	IP address or IP address range for the pool.
Single ports	Number of allocated single ports.
Twin ports	Number of allocated twin ports.

Copyright © 2011, Juniper Networks, Inc.

show security nat source pool src-nat-pool1

```
user@host> show security nat source pool src-nat-pool1
    Pool name:         src-nat-pool1
    Pool id:           1
    Routing instance:  ri-1
    Port range:        [2000,63000]
    Total address:     1
    Address available: 1
    Address range              Single ports Twin ports
    30.30.30.6-30.30.30.6                 0          0
```

show security nat source pool all

```
user@host> show security nat source pool all
    Total source nat pool number: 2
    Pool name:         src-nat-pool1
    Pool id:           1
    Routing instance:  ri-1
    Port range:        [2000,63000]
    Total address:     1
    Address available: 1
    Address range              Single ports Twin ports
    30.30.30.6-30.30.30.6                 0          0
    Pool name:         src-nat-pool2
    Pool id:           2
    Routing instance:  ri-1
    Port translation:  no
    Total address:     81
    Address available: 50
    Address range              Single ports Twin ports
    10.0.0.20-10.0.0.100                  0          0
```


Copyright © 2011, Juniper Networks, Inc.

show security nat source rule

Syntax

show security nat source rule
<rule-name>
all

Release Information

Command introduced in Release 9.2 of Junos OS.

Description

Display information about the specified source Network Address Translation (NAT) rule.

Options

rule-name—Name of the rule.

all—Display information about all the source NAT rule.

Required Privilege Level

view

Related Documentation

- **rule (Source NAT) on page 684**

List of Sample Output

show security nat source rule r1 on page 1520
show security nat source rule all on page 1520

Output Fields

Table 146 on page 1519 lists the output fields for the show security nat source rule command. Output fields are listed in the approximate order in which they appear

Table 146: show security nat source rule Output Fields

Field Name	Field Description
Source nat rule	Name of the source NAT rule.
State	Status of the IP address: • **Active**—Denotes that the IP address is in use. • **Free**—IP address is available for allocation.
Index	Rule index number.
From routing instance	Name of the routing instance from which the packet comes.
To routing instance	Name of the routing instance in which packet should reach.
Source address	Name of the source addresses which match the rule. The default value is any.
Destination address	Name of the destination addresses which match the rule. The default value is any.
Destination ports	Destination ports number which match the rule. The default value is any.

Copyright © 2011, Juniper Networks, Inc.

Table 146: show security nat source rule Output Fields *(continued)*

Field Name	Field Description
Action	The action taken in regard to a packet that matches the rule's tuples. Actions include the following: • **off**—Do not perform source NAT. • **source-nat**—Use user-defined source NAT pool to perform source NAT • **interface**—Use egress interface's IP address to perform source NAT.
Hit times	Number of times a translation in the translation table is used for a source NAT rule.
Fail times	Number of times a translation in the translation table failed to translate for a source NAT rule.
Total destination nat rule number	Number of destination NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the source NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the source NAT rules.

show security nat source rule r1

```
user@host> show security nat source rule r1
    Source nat rule: r1, State: enabled, Index: 4
      From routing instance: ri-2
      To routing instance: ri-1
      Source addresses:
        any: 0.0.0.0/0
      Destination addresses:
        any: 0.0.0.0/0
      Action: source-nat pool s1

      Hit times: 22
      Fail times: 2
```

show security nat source rule all

```
user@host> show security nat source rule all
    Total source nat rule number: 2
    Total hit times: 32
    Total fail times: 2

    Source nat rule: r1, State: enabled, Index: 4
      From routing instance: ri-2
      To routing instance: ri-1
      Source addresses:
        any: 0.0.0.0/0
      Destination addresses:
        any: 0.0.0.0/0
      Action: source-nat pool s1

      Hit times: 22
      Fail times: 2

    Source nat rule: r2, State: enabled, Index: 5
      From routing instance: ri-2, zone: z3 z4
      To routing instance: ri-1
```


Copyright © 2011, Juniper Networks, Inc.

```
Source addresses:
  any: 0.0.0.0/0
Destination addresses:
  any: 0.0.0.0/0
Action: source-nat pool s2

Hit times: 10
Fail times: 0
```

show security nat source summary

Syntax show security nat source summary

Release Information Command introduced in Release 9.2 of Junos OS.

Description Display a summary of Network Address Translation (NAT) source pool information.

Required Privilege Level view

Related Documentation
- **pool (Source NAT) on page 626**
- **rule (Source NAT) on page 684**

List of Sample Output **show security nat source summary on page 1522**

Output Fields Table 147 on page 1522 lists the output fields for the **show security nat source summary** command. Output fields are listed in the approximate order in which they appear.

Table 147: show security nat source summary Output Fields

Field Name	Field Description
Total source nat pool number	Number of source NAT pools.
Pool name	Name of the source address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
PAT IP	Whether Port Address Translation (PAT) is enabled (yes or no).
total IP	Number of IP addresses that are in use.
available	Number of IP addresses that are free for use.
Total source nat rule number	Number of source NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the source NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the source NAT rules.

show security nat source summary

```
user@host> show security nat source summary
    Total source nat pool number: 2
    Pool name      Address range   Routing instance PAT IP total IP available
    src-nat-pool1 30.30.30.6-30.30.30.6   ri-1      yes    1         1
    src-nat-pool2 10.0.0.20-10.0.0.100    ri-1       no   81        50
```


Copyright © 2011, Juniper Networks, Inc.

```
Total source nat rule number: 1
Total hit times: 22
Total fail times: 2
```

show security nat static rule

Syntax

show security nat static rule
<rule-name>
all

Release Information

Command introduced in Release 9.3 of Junos OS.

Description

Display information about the specified static Network Address Translation (NAT) rule.

Options

rule-name —Name of the rule.

all—Display information about all the static NAT rules.

Required Privilege Level

view

Related Documentation

- **rule (Static NAT) on page 685**

List of Sample Output

show security nat static rule rsr11 on page 1525
show security nat static rule all on page 1525

Output Fields

Table 148 on page 1524 lists the output fields for the **show security nat static rule** command. Output fields are listed in the approximate order in which they appear.

Table 148: show security nat static rule Output Fields

Field Name	Field Description
Static nat rule	Name of the static NAT rule.
Rule-set	Name of the rule-set. Currently, you can configure 8 rules within the same rule-set.
Rule-Id	Rule ID number.
Rule-position	Position of the rules indicates the order that they apply to traffic.
From interface	Name of the interface from which the packet comes.
From routing instance	Name of the routing instance from which the packet comes.
Destination address	Name of the destination addresses that match the rule.
Host addresses	Name of the host addresses that match the rule.
Netmask	Subnet IP address.
Translation hits	Number of times a translation in the translation table is used for a static NAT rule.

Copyright © 2011, Juniper Networks, Inc.

show security nat static rule rsr11

```
user@host> show security nat static rule rsr11
Static NAT rule: rsr11              Rule-set: rsr1
  Rule-Id                    : 1
  Rule position              : 4
  From routing instance      : default
  Destination addresses      : 40.0.0.0
  Host addresses             : 31.0.0.0
  Netmask                    : 255.255.255.0
  Translation hits           : 0
```

show security nat static rule all

```
user@host> show security nat static rule all
Static NAT rule: rsr3               Rule-set: rsr2
  Rule-Id                    : 3
  Rule position              : 6
  From interface             : ge-0/0/1.0
  Destination addresses      : 60.0.0.0
  Host addresses             : 100.0.0.0
  Netmask                    : 255.255.255.0
  Translation hits           : 0
Static NAT rule: rsr11              Rule-set: rsr1
  Rule-Id                    : 1
  Rule position              : 4
  From routing instance      : default
  Destination addresses      : 40.0.0.0
  Host addresses             : 31.0.0.0
  Netmask                    : 255.255.255.0
  Translation hits           : 0
```

Copyright © 2011, Juniper Networks, Inc.

show security nat static-nat summary

Syntax

show security nat static-nat summary
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display static Network Address Translation (NAT) summary information.

Options

none—Display static NAT summary information.

node—(Optional) For chassis cluster configurations, display static NAT summary information on specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security nat static-nat summary on page 1526

Output Fields

Table 149 on page 1526 lists the output fields for the **show security nat static-nat summary** command. Output fields are listed in the approximate order in which they appear.

Table 149: show security nat static-nat summary Output Fields

Field Name	Field Description
Total static NAT mappings	Number of static NAT entries in the table.
Maximum	Maximum number of static NAT entries possible.
Ingress Interface	Name of the interface on which static NAT is defined.
Destination	Destination IP address and subnet mask.
Host	Host IP address and subnet mask mapped to the destination IP address and subnet mask.
Virtual Router	Name of the virtual device that performs route lookup for the host IP address and subnet mask.

show security nat static-nat summary

```
user@host> show security nat static-nat summary
  Total static NAT mappings: 3, Maximum: 300
  Ingress Interface    Destination    Host         Virtual Router
  ge-0/0/0.0           1.1.1.1/32     10.1.1.1/32  trust-vr
```


Copyright © 2011, Juniper Networks, Inc.

```
ge-0/0/0.0          1.1.3.0/24     10.1.3.0/24  trust-vr
ge-0/0/0.1          2.2.2.1/32     20.1.1.1/32  trust-vr
```

show security pki ca-certificate

Syntax

show security pki ca-certificate
<**brief** | **detail**>
<**ca-profile** *ca-profile-name* >

Release Information

Command modified in Release 8.5 of Junos OS.

Description

Display information about the certificate authority (CA) public key infrastructure (PKI) digital certificates configured on the device.

Options

none—Display basic information about all configured CA certificates.

brief | **detail**—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*- (Optional) Display information about only the specified CA certificate.

Required Privilege Level

view

Related Documentation

- **ca-profile on page 365**
- **request security pki ca-certificate verify on page 1113**
- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show security pki ca-certificate ca-profile juniper brief on page 1529
show security pki ca-certificate ca-profile juniper detail on page 1530

Output Fields

Table 150 on page 1528 lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 150: show security pki ca-certificate Output Fields

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Serial number	Unique serial number of the digital certificate.
Issued to	Device that was issued the digital certificate.
Issued by	Authority that issued the digital certificate.

Copyright © 2011, Juniper Networks, Inc.

Table 150: show security pki ca-certificate Output Fields *(continued)*

Field Name	Field Description
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**).
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.
Fingerprint	Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate.
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**.

show security pki ca-certificate ca-profile juniper brief

```
user@host> show security pki ca-certificate ca-profile juniper brief
  Certificate identifier: kpradeep.juniper.net
    Issued to: kpradeep.juniper.net, Issued by: kpradeep.juniper.net
    Validity:
      Not before: 2005 Jul  8th, 12:44:54 GMT
      Not after: 2010 Jul  8th, 12:46:07 GMT
    Public key algorithm: rsaEncryption(1024 bits)
  Certificate identifier: kpradeep.juniper.net
    Issued to: kpradeep.newra.juniper.net, Issued by: kpradeep.juniper.net
    Validity:
      Not before: 2005 Jul 12th, 12:48:32 GMT
      Not after: 2006 Jul 12th, 12:58:32 GMT
    Public key algorithm: rsaEncryption(1024 bits)
```

```
  Certificate identifier: kpradeep.juniper.net
    Issued to: kpradeep.newra.juniper.net, Issued by: kpradeep.juniper.net
    Validity:
      Not before: 2005 Jul 12th, 12:48:32 GMT
      Not after: 2006 Jul 12th, 12:58:32 GMT
    Public key algorithm: rsaEncryption(1024 bits)
```

show security pki ca-certificate ca-profile juniper detail

```
user@host> show security pki ca-certificate ca-profile juniper detail
Certificate identifier: kpradeep.juniper.net
    Certificate version: 3
    Serial number: 1442 8439 1974 7864 6894 2623 4704 6564 1574
    Issuer:
      Common name: kpradeep.juniper.net
    Subject:
      Common name: kpradeep.juniper.net
    Validity:
      Not before: 2005 Jul  8th, 12:44:54 GMT
      Not after: 2010 Jul  8th, 12:46:07 GMT
    Public key algorithm: rsaEncryption(1024 bits)
      e8:ba:49:61:42:c4:3e:81:07:19:8d:cd:38:cc:85:9b:ff:d2:c6:90:04:fa
      18:58:8a:03:59:57:3d:b2:f0:06:62:a7:93:db:4e:8c:5d:6d:14:80:4e:38
      03:69:64:ac:56:cf:72:d7:49:d1:00:45:c8:02:68:fd:e0:af:98:78:b1:b9
      ee:9c:ad:21:f2:9d:7b:06:c4:71:b2:be:f4:e3:58:af:22:3b:ae:dc:1a:5e
      f2:35:2c:0b:49:23:ee:2e:ba:e4:9a:24:f3:ff:01:5c:20:92:1d:76:51:fb
      6b:bb:45:65:2f:db:2b:d7:e5:7d:03:9b:3e:21:88:75:46:5f
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
      71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
    Distribution CRL:
      file://\\multiplex\CertEnroll\kpradeep.juniper.net.crl
      http://multiplex/CertEnroll/kpradeep.juniper.net.crl
    Use for key: CRL signing, Certificate signing, Digital signature
  Certificate identifier: kpradeep.juniper.net
    Certificate version: 3
    Serial number: 9998 7697 0440 0585 1234
    Issuer:
      Common name: kpradeep.juniper.net
    Subject:
      Organization: Juniper Networks, Organizational unit: Pepsi, Country: IN,
      Locality: Bangalore, Common name: kpradeep.newra.juniper.net
    Validity:
      Not before: 2005 Jul 12th, 12:48:32 GMT
      Not after: 2006 Jul 12th, 12:58:32 GMT
    Public key algorithm: rsaEncryption(1024 bits)
      bd:26:77:95:16:23:b4:82:fc:cd:ea:fe:28:41:d4:d3:fd:df:f7:76:03:a6
      23:3a:8a:6e:9e:25:41:e3:96:57:4a:bf:dc:5e:f2:09:a6:07:79:02:f7:40
      1b:b9:79:70:79:65:c8:70:d9:6a:bd:a9:9c:cd:b3:39:80:e5:5a:c7:74:66
      4a:05:b7:3b:ed:7a:99:e9:4b:58:e6:e7:69:9a:79:d4:c1:a5:26:12:5e:8d
      3b:d1:b0:22:df:a9:ba:a2:23:73:21:1b:62:44:72:ad:c0:c3:7c:56:e8:ea
      fe:ae:81:2b:44:8b:fe:da:ea:e3:18:85:bf:05:ea:28:8d:4b
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
      ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
    Distribution CRL:
      file://\\multiplex\CertEnroll\kpradeep.juniper.net.crl
      http://multiplex/CertEnroll/kpradeep.juniper.net.crl
    Use for key: Data encipherment, Key encipherment
  Certificate identifier: kpradeep.juniper.net
    Certificate version: 3
```


Copyright © 2011, Juniper Networks, Inc.

```
Serial number: 9998 7666 0817 5841 3062
Issuer:
  Common name: kpradeep.juniper.net
Subject:
  Organization: Juniper Networks, Organizational unit: Pepsi,
                    Country: IN,
  Locality: Bangalore, Common name: kpradeep.newra.juniper.net
Validity:
  Not before: 2005 Jul 12th, 12:48:32 GMT
  Not after: 2006 Jul 12th, 12:58:32 GMT
Public key algorithm: rsaEncryption(1024 bits)
  b6:b8:70:5f:c5:c5:c4:6d:be:a5:1e:19:12:b2:d4:8f:44:01:89:aa:66:98
  2d:21:0c:a2:45:04:ac:09:f6:8f:c7:ae:c3:40:d7:f4:b7:d8:8f:f1:21:d0
  c5:f0:b4:ea:05:c6:92:3a:e6:2e:33:0f:7b:a0:e1:de:16:52:13:09:16:91
  01:4a:bb:1e:f5:8d:98:e1:e4:2a:03:81:46:4f:1a:a3:20:4e:4d:5c:6e:f5
  ab:7e:08:81:b3:c0:78:2d:7b:ae:be:db:56:1e:6d:34:1f:a3:20:6e:7f:59
  a0:f1:d6:52:d9:35:5d:0a:f6:b4:ef:97:47:5b:0e:d3:11:2b
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
  23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
  file://\\multiplex\CertEnroll\kpradeep.juniper.net.crl
  http://multiplex/CertEnroll/kpradeep.juniper.net.crl
Use for key: Non repudiation, Digital signature
```

show security pki certificate-request

Syntax

show security pki certificate-request
<**brief | detail**>
<certificate-id *certificate-id-name* >

Release Information

Command modified in Release 8.5 of Junos OS.

Description

Display information about manually generated local digital certificate requests that are stored on the device.

Options

none—Display basic information about all local digital certificate requests.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified local digital certificate requests.

Required Privilege Level

view

Related Documentation

- **clear security pki key-pair on page 1077**
- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show security pki certificate-request certificate-id hassan brief on page 1533
show security pki certificate-request certificate-id hassan detail on page 1533

Output Fields

Table 151 on page 1532 lists the output fields for the **show security pki certificate-request** command. Output fields are listed in the approximate order in which they appear.

Table 151: show security pki certificate-request Output Fields

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Issued to	Device that was issued the digital certificate.
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Alternate subject	Domain name or IP address of the device related to the digital certificate.

Copyright © 2011, Juniper Networks, Inc.

Table 151: show security pki certificate-request Output Fields *(continued)*

Field Name	Field Description
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**).
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.
Fingerprint	Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate.
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**.

show security pki certificate-request certificate-id hassan brief

```
user@host> show security pki certificate-request certificate-id hassan brief
Certificate identifier: hassan
      Issued to: hassan@juniper.net
      Public key algorithm: rsaEncryption(1024 bits)
```

show security pki certificate-request certificate-id hassan detail

```
user@host> show security pki certificate-request certificate-id hassan detail
    Certificate identifier: hassan
      Certificate version: 3
      Subject:
        Organization: juniper, Organizational unit: pepsi, Country: IN,
                        Common name: hassan
      Alternate subject: 102.168.72.124
      Public key algorithm: rsaEncryption(1024 bits)
      Public key verification status: Passed
        c7:a4:fb:e7:8c:4f:31:e7:eb:01:d8:32:65:21:f2:eb:6f:7d:49:1a:c3:9b
        63:47:e2:4f:f6:db:f6:c8:75:dd:e6:ec:0b:35:0a:62:32:45:6b:35:1f:65
        c9:66:b7:40:b2:f9:2a:ab:5b:60:f7:c7:73:36:da:68:25:fc:40:4b:12:3c
        d5:c8:c6:66:f6:10:1e:86:67:a8:95:9b:7f:1c:ae:a7:55:b0:28:95:a7:9a
        a2:24:28:e4:5a:b2:a9:06:7a:69:37:20:15:e1:b6:66:eb:22:b5:b6:77:f6
        65:88:b0:94:2b:91:4b:99:78:4a:e3:56:cc:14:45:d7:97:fd
      Fingerprint:
        8f:22:1a:f2:9f:27:b0:21:6c:da:46:64:31:34:1f:68:42:5a:39:e0 (sha1)
        09:15:11:aa:ea:f9:5a:b5:70:d7:0b:8e:be:a6:d3:cb (md5)
      Use for key: Digital signature
```

show security pki crl

Syntax

show security pki crl
< **brief** | **detail**>
<ca-profile *ca-profile-name* >

Release Information

Command modified in Release 8.5 of Junos OS.

Description

Display information about the certificate revocation lists (CRLs) configured on the device.

Options

none—Display basic information about all CRLs.

brief | **detail**—(Optional) Display the specified level of output.

ca-profile ***ca-profile-name-*** (Optional) Display information about only the specified CA profile.

Required Privilege Level

view

Related Documentation

- **crl on page 383**
- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show security pki crl ca-profile ca2 on page 1535
show security pki crl ca-profile ca2 brief on page 1535
show security pki crl ca-profile ca2 detail on page 1535

Output Fields

Table 152 on page 1534 lists the output fields for the **show security pki crl** command. Output fields are listed in the approximate order in which they appear.

Table 152: show security pki crl Output Fields

Field Name	Field Description
CA profile	Name of the configured CA profile.
CRL version	Revision number of the certificate revocation list.
CRL issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **emailAddress**—Mail address of the issuing authority. • **C**—Country of origin. • **ST**—State of origin. • **L**—Locality of origin. • **O**—Organization of origin. • **OU**—Department within an organization. • **CN**—Name of the authority.
Effective date	Date and time the certificate revocation list becomes valid.

Copyright © 2011, Juniper Networks, Inc.

Table 152: show security pki crl Output Fields *(continued)*

Field Name	Field Description
Next update	Date and time the routing platform will download the latest version of the certificate revocation list.
Revocation List	List of digital certificates that have been revoked before their expiration date. Values are: • **Serial number**—Unique serial number of the digital certificate. • **Revocation date**—Date and time that the digital certificate was revoked.

show security pki crl ca-profile ca2

```
user@host> show security pki crl ca-profile ca2
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
```

show security pki crl ca-profile ca2 brief

```
user@host> show security pki crl ca-profile ca2 brief
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
```

show security pki crl ca-profile ca2 detail

```
user@host> show security pki crl ca-profile ca2 detail
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
  Revocation List:
    Serial number              Revocation date
    174e6399000000000506       03-16-2007 23:09
    174ef3f3000000000507       03-16-2007 23:09
    17529cd6000000000508       03-16-2007 23:09
    1763ac26000000000509       03-16-2007 23:09
    21904e5700000000050a       03-16-2007 23:09
    2191cf7900000000050b       03-16-2007 23:09
    21f10eb600000000050c       03-16-2007 23:09
    2253ca2a00000000050f       03-16-2007 23:09
    2478939b000000000515       03-16-2007 23:09
    24f35004000000000516       03-16-2007 23:09
    277ddfa8000000000517       03-16-2007 23:09
    277e97bd000000000518       03-16-2007 23:09
    27846a76000000000519       03-16-2007 23:09
    2785176f00000000051a       03-16-2007 23:09
```

Copyright © 2011, Juniper Networks, Inc.

show security pki local-certificate

Syntax

show security pki local-certificate
< **brief** | **detail** >
< certificate-id *certificate-id-name* >
<system-generated>

Release Information

Command modified in Release 9.1 of Junos OS.

Description

Display information about the local digital certificates, corresponding public keys, and the automatically generated self-signed certificate configured on the device.

Options

none—Display basic information about all configured local digital certificates, corresponding public keys, and the automatically generated self-signed certificate.

brief | **detail**—(Optional) Display the specified level of output.

certificate-id ***certificate-id-name***—(Optional) Display information about only the specified local digital certificates and corresponding public keys.

system-generated—Display information about the automatically generated self-signed certificate.

Required Privilege Level

view

Related Documentation

- **clear security pki local-certificate on page 1078**
- **request security pki local-certificate generate-self-signed on page 1114**
- *Junos OS System Basics and Services Command Reference*

List of Sample Output

show security pki local-certificate certificate-id on page 1537
show security pki local-certificate certificate-id detail on page 1538
show security pki local-certificate system-generated on page 1538
show security pki local-certificate system-generated detail on page 1538

Output Fields

Table 153 on page 1536 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 153: show security pki local-certificate Output Fields

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Serial number	Unique serial number of the digital certificate.
Issued to	Device that was issued the digital certificate.

Copyright © 2011, Juniper Networks, Inc.

Table 153: show security pki local-certificate Output Fields *(continued)*

Field Name	Field Description
Issued by	Authority that issued the digital certificate.
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **Country**—Country of origin. • **Locality**—Locality of origin. • **Common name**—Name of the authority.
Alternate subject	Domain name or IP address of the device related to the digital certificate.
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**).
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.
Fingerprint	Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate.
Distribution CRL	Distinguished name information and URL for the certificate revocation list (**CRL**) server.
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**.

show security pki local-certificate certificate-id

```
user@host> show security pki local-certificate certificate-id hassan
   Certificate identifier: hassan
     Issued to: hassan, Issued by: kpradeep.juniper.net
     Validity:
       Not before: 2005 Aug  2nd, 05:23:42 GMT
       Not after: 2006 Aug  2nd, 05:33:42 GMT
```

```
    Public key algorithm: rsaEncryption(1024 bits)
    Public key verification status: Passed
```

show security pki local-certificate certificate-id detail

```
user@host> show security pki local-certificate certificate-id hassan detail
   Certificate identifier: hassan
    Certificate version: 3
    Serial number: 3115 8938 6334 6035 7529
    Issuer:
      Common name: kpradeep.juniper.net
    Subject:
      Organization: juniper, Organizational unit: pepsi, Country: IN,
                        Common name: hassan
    Alternate subject: hassan.com
    Validity:
       Not before: 2005 Aug  2nd, 05:23:42 GMT
       Not after: 2006 Aug  2nd, 05:33:42 GMT
    Public key algorithm: rsaEncryption(1024 bits)
    Public key verification status: Passed
      c7:a4:fb:e7:8c:4f:31:e7:eb:01:d8:32:65:21:f2:eb:6f:7d:49:1a:c3:9b
      63:47:e2:4f:f6:db:f6:c8:75:dd:e6:ec:0b:35:0a:62:32:45:6b:35:1f:65
      c9:66:b7:40:b2:f9:2a:ab:5b:60:f7:c7:73:36:da:68:25:fc:40:4b:12:3c
      d5:c8:c6:66:f6:10:1e:86:67:a8:95:9b:7f:1c:ae:a7:55:b0:28:95:a7:9a
      a2:24:28:e4:5a:b2:a9:06:7a:69:37:20:15:e1:b6:66:eb:22:b5:b6:77:f6
      65:88:b0:94:2b:91:4b:99:78:4a:e3:56:cc:14:45:d7:97:fd
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      36:ec:35:5a:9a:6d:1c:77:a8:bb:f6:b9:94:57:36:11:c8:88:93:cc (sha1)
      1f:ab:f2:a0:84:5a:9c:e6:0e:92:79:70:cf:2c:1a:73 (md5)
   Distribution CRL:
     file://\\multiplex\CertEnroll\kpradeep.juniper.net.crl
     http://multiplex/CertEnroll/kpradeep.juniper.net.crl
    Use for key: Digital signature
```

show security pki local-certificate system-generated

```
user@host> show security pki local-certificate system-generated
Certificate identifier: system-generated
  Issued to: JN10D3DFCADA, Issued by: CN = JN10D3DFCADA, CN = system generated,
CN = self-signed
  Validity:
    Not before: 02-21-2008 10:27
    Not after: 02-19-2013 10:27
  Public key algorithm: rsaEncryption(1024 bits)
```

show security pki local-certificate system-generated detail

```
user@host> show security pki local-certificate system-generated detail
Certificate identifier: system-generated
  Certificate version: 3
  Serial number: a3f42347afe6953f8f3fe4aae70f310f
  Issuer:
    Common name: JN10D3DFCADA
  Subject:
    Common name: JN10D3DFCADA
  Alternate subject: email empty, fqdn empty, ip empty
  Validity:
    Not before: 02-21-2008 10:27
    Not after: 02-19-2013 10:27
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:c1:50:fa:46:eb:57:6b:7d:11:05:a0:7d:17
    0c:2b:0e:d1:26:4c:ae:4d:75:b2:c9:73:2d:bb:d0:ef:07:f0:24:9e
    23:42:29:79:30:c3:3b:f4:b7:5a:74:3a:9c:d1:66:45:af:e8:41:5d
    52:bf:81:c3:c9:d9:d5:ba:0f:5e:d3:28:d4:44:d2:60:0c:42:76:c5
    ed:93:89:20:13:ee:e6:23:ab:d6:e5:fe:5e:13:a2:94:c0:ae:f9:1e
```


Copyright © 2011, Juniper Networks, Inc.

```
  cd:fa:ca:9f:59:92:b4:b3:84:e9:61:76:7b:81:f4:5a:48:a6:91:ae
  39:99:b9:3a:06:ac:d7:b2:15:85:bd:8f:b7:90:e1:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  42:79:b0:f0:fa:fc:03:33:bd:0d:d4:56:21:f1:d9:28:51:00:3f:b0 (sha1)
  f0:77:8e:3e:1d:41:12:a1:bf:3d:cd:19:e5:66:3e:15 (md5)
```

show security policies

Syntax

show security policies
<detail>
<policy-name *policy-name*>

Release Information

Command modified in Release 9.2 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS and support for IPv6 addresses in active/active chassis cluster configurations in addition to the existing support of active/passive chassis cluster configurations added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS.

Description

Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.

Options

none—Display basic information about all configured policies.

detail—(Optional) Display a detailed view of all of the policies configured on the device.

policy-name *policy-name*—(Optional) Display information about the specified policy.

Required Privilege Level

view

Related Documentation

- **clear security policies statistics on page 1079**

List of Sample Output

show security policies on page 1542
show security policies policy-name p1 detail on page 1543

Output Fields

Table 154 on page 1540 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 154: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.

Copyright © 2011, Juniper Networks, Inc.

Table 154: show security policies Output Fields *(continued)*

Field Name	Field Description
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The IP protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0. • **Inactivity timeout**: Elapse time without activity after which the application is terminated. • **Source port range**: The low-high source port range for the session application.
Destination Address Translation	Status of the destination address translation traffic: • drop translated— Drop the packets with translated destination address. • drop untranslated—Drop the packets without translated destination address.

Action or Action-type	• The action taken in regard to a packet that matches the policy's tuples. Actions include the following:
	  • **permit**
	  • **firewall-authentication**
	  • **tunnel ipsec-vpn** *vpn-name*
	  • **pair-policy** *pair-policy-name*
	  • **source-nat pool pool-name**
	  • **pool-set** *pool-set-name*
	  • **interface**
	  • **destination-nat** *name*
	  • **deny**
	  • **reject**

Index	An internal number associated with the policy.
Session log	Session log entry that indicates whether the **at-create** and **at-close** flags were set at configuration time to log session information.

Copyright © 2011, Juniper Networks, Inc.

Table 154: show security policies Output Fields *(continued)*

Field Name	Field Description
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active (or inactive) to check an incoming packet to determine how to treat the packet.
Policy statistics	Policy statistics include the following: • **Input bytes**—The number of bytes presented for processing by the device. • **Output bytes**—The number of bytes actually processed by the device. • **Input packets**—The number of packets presented for processing by the device. • **Active sessions**—The number of sessions currently present because of access control lookups that used this policy. • **Session deletions**—The number of sessions deleted since system startup. • **Policy lookups**—Number of times the policy was accessed to check for a match. NOTE: Configure the Policy P1 with **count** option to display policy statistics.

Application Firewall	Application Firewall include the following:
	• **Rule-set**—Name of the rule set.
	• **Rule**—Name of the rule.
	  ◦ **Dynamic applications**—Name of the applications.
	  ◦ **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ◦ **permit**
	  ◦ **deny**
	• **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set.

show security policies

```
user@host> show security policies
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Sequence number: 1
    Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
    Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
    Applications: any
    Action: permit, application services, log, scheduled
    Application firewall : my_ruleset1
  Policy: p2, State: enabled, Index: 5, Sequence number: 2
    Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
  Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
```


Copyright © 2011, Juniper Networks, Inc.

```
    da-3-ipv6: 2400:0d78:0/24
    Applications: any
    Action: deny, scheduled
```

show security policies policy-name p1 detail

```
user@host> show security policies policy-name p1 detail
show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
  Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Destination Address Translation: drop translated
  Application firewall :
  Rule-set: my_ruleset1
    Rule: rule1
      Dynamic Applications: junos:FACEBOOK, junos:YSMG
      Action: deny
    Default rule: permit
  Session log: at-create, at-close
  Scheduler name: sch20
  Policy statistics:
    Input  bytes     :                50000                  100 bps
    Output bytes     :                40000                  100 bps
    Input  packets   :                  200                  200 pps
    Output packets   :                  100                  100 pps
    Session rate     :                    2                    1 sps
    Active sessions  :                   11
    Session deletions:                   20
    Policy lookups   :                   12
```

show security resource-manager group active

Syntax

show security resource-manager group active
<group-number >
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display security information about active groups created through the resource manager.

Options

none—Display resource manager group service information for all active groups.

group-number —(Optional) Display resource manager group service information for a specific group identification number.

node—(Optional) For chassis cluster configurations, display active resource manager group service information on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security resource-manager group active on page 1544
show security resource-manager group active 2048 on page 1545
show security resource-manager group active node primary on page 1545
show security resource-manager group active node all on page 1545
show security resource-manager group active 1024 node all on page 1545

Output Fields

Table 155 on page 1544 lists the output fields for the **show security resource-manager group** command. Output fields are listed in the approximate order in which they appear.

Table 155: show security resource-manager group Output Fields

Field Name	Field Description
Total groups	Total number of groups in the system.
active groups	Number of active groups.
Group ID	Identification number whose group information is displayed.

show security resource-manager group active

```
user@host> show security resource-manager group active
Total groups 32, active groups 0
```


Copyright © 2011, Juniper Networks, Inc.

show security resource-manager group active 2048

```
user@host> show security resource-manager group active 2048
Total groups 2048, active groups 1
Group ID 2048: state - Active
          : Virtual System      - root
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8190
               Resource ID - 8188
               Resource ID - 8187
```

show security resource-manager group active node primary

```
user@host> show security resource-manager group active node primary
node0:
--------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

show security resource-manager group active node all

```
user@host> show security resource-manager group active node all
node0:
--------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
node1:
--------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

show security resource-manager group active 1024 node all

```
user@host> show security resource-manager group active 1024 node all
node0:
--------------------------------------------------------------------------
Group ID 1024: state - Active
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8192
               Resource ID - 8188
               Resource ID - 8187
node1:
--------------------------------------------------------------------------
Group ID 1024: state - Active
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8187
               Resource ID - 8186
               Resource ID - 8190
```

show security resource-manager resource active

Syntax

show security resource-manager resource **active**
<resource-id >
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display security information about active resources created through the resource manager.

Options

none—Display information for all active resources.

resource-id —(Optional) Display information for a resource with a specific identification number.

node—(Optional) For chassis cluster configurations, display active resource manager information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security resource-manager resource active on page 1546
show security resource-manager resource active 8190 on page 1547
show security resource-manager resource active node local on page 1547
show security resource-manager resource active node primary on page 1547

Output Fields

Table 156 on page 1546 lists the output fields for the **show security resource-manager resource** command. Output fields are listed in the approximate order in which they appear.

Table 156: show security resource-manager resource Output Fields

Field Name	Field Description
Total resources	Total number of resources in the system.
active resources	Number of active resources.
Resource ID	Identification number whose resource information is displayed.

show security resource-manager resource active

```
user@host> show security resource-manager resource active
Total resources 128, active resources 0
```


Copyright © 2011, Juniper Networks, Inc.

show security resource-manager resource active 8190

```
user@host> show security resource-manager resource active 8190
Total resource 8192, active resource 3
Resource ID 8190: state - Active
          : Start time          - 0
          : Resource timeout    - 120
          : Parent group        - 2048
          : Number of sessions  - 1
               Session ID - 8
          : Number of Holes  - 1
               1) Source IP Range        - {0.0.0.0, 0.0.0.0}
                  Source Port Range      - {0, 0}
                  Destination IP Range   - {20.20.20.31, 20.20.20.31}
                  Destination Port Range - {50195, 50195}
                  Protocol               - 17
                  Reference count        - 1
```

show security resource-manager resource active node local

```
user@host> show security resource-manager resource active node local
node0:
--------------------------------------------------------------------------
    Resource ID 8192: Group ID - 1024, Application - SIP ALG
    Resource ID 8188: Group ID - 1024, Application - SIP ALG
    Resource ID 8187: Group ID - 1024, Application - SIP ALG
Total Resources 8192, active resources 3
```

show security resource-manager resource active node primary

```
user@host> show security resource-manager resource active node primary
node0:
--------------------------------------------------------------------------
    Resource ID 8192: Group ID - 1024, Application - SIP ALG
    Resource ID 8188: Group ID - 1024, Application - SIP ALG
    Resource ID 8187: Group ID - 1024, Application - SIP ALG
Total Resources 8192, active resources 3
```

show security resource-manager settings

Syntax

show security resource-manager settings
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display resource manager settings.

Options

node—(Optional) For chassis cluster configurations, display resource manager settings on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

List of Sample Output

show security resource-manager settings on page 1548
show security resource-manager settings node primary on page 1548
show security resource-manager settings node all on page 1549

Output Fields

Table 157 on page 1548 lists the output fields for the **show security resource-manager settings** command. Output fields are listed in the approximate order in which they appear.

Table 157: show security resource-manager settings Output Fields

Field Name	Field Description
Client Heartbeat	Time after which idle an resource manager client is timed out.
Count	Number of active clients.
Pinhole age	Duration for which the temporary opening in the security firewall (pinhole) is open for specified traffic. If the specified traffic does not exist during this time period, the pinhole is timed out.

show security resource-manager settings

```
user@host> show security resource-manager settings
Client Heartbeat: timeout 600 seconds, count 5
Pinhole age: 32 seconds
```

show security resource-manager settings node primary

```
user@host> show security resource-manager settings node primary
node0:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
```


Copyright © 2011, Juniper Networks, Inc.

show security resource-manager settings node all

```
user@host> show security resource-manager settings node all
node0:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
node1:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
```

show security screen ids-option

Syntax

show security screen ids-option
screen-name
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display configuration information about the specified security screen.

Options

screen-name —Name of the screen.

node—(Optional) For chassis cluster configurations, display the configuration status of the security screen on a specific node.

- *node-id* —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **ids-option on page 504**

List of Sample Output

show security screen ids-option jscreen on page 1551
show security screen ids-option jscreen1 node all on page 1551

Output Fields

Table 158 on page 1550 lists the output fields for the **show security screen ids-option** command. Output fields are listed in the approximate order in which they appear.

Table 158: show security screen ids-option Output Fields

Field Name	Field Description
TCP address sweep threshold	Number of microseconds for which the device accepts 10 TCP packets from the same remote source to different destination addresses.
TCP port scan threshold	Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers.
ICMP address sweep threshold	Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device.
UDP flood threshold	Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.
TCP winnuke	Enable or disable the detection of TCP WinNuke attacks.

Copyright © 2011, Juniper Networks, Inc.

Table 158: show security screen ids-option Output Fields *(continued)*

Field Name	Field Description
TCP SYN flood attack threshold	Number of SYN packets per second required to trigger the SYN proxy response.
TCP SYN flood alarm threshold	Number of half-complete proxy connections per second at which the device makes entries in the event alarm log.
TCP SYN flood source threshold	Number of SYN segments to be received per second before the device begins dropping connection requests.
TCP SYN flood destination threshold	Number of SYN segments received per second before the device begins dropping connection requests.
TCP SYN flood timeout	Maximum length of time before a half-completed connection is dropped from the queue.
TCP SYN flood queue size	Number of proxy connection requests that can be held in the proxy connection queue before the device begins rejecting new connection requests.
ICMP large packet	Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes.
UDP address sweep threshold	Number of microseconds for which the device accepts 10 UDP packets from the same remote source to different destination addresses.

show security screen ids-option jscreen

```
user@host> show security screen ids-option jscreen
Screen object status:
Name                                        Value
  TCP port scan threshold                   5000
  ICMP address sweep threshold              5000
```

show security screen ids-option jscreen1 node all

```
user@host>  show security screen ids-option jscreen1 node all
node0:
--------------------------------------------------------------------------
Screen object status:
Name                                        Value
  UDP flood threshold                       1000
  TCP winnuke                               enabled
  TCP SYN flood attack threshold            200
  TCP SYN flood alarm threshold             512
  TCP SYN flood source threshold            4000
  TCP SYN flood destination threshold       4000
  TCP SYN flood timeout                     20
  TCP SYN flood queue size                  1024
  ICMP large packet                         enabled
node1:
--------------------------------------------------------------------------
Screen object status:
Name                                        Value
  UDP flood threshold                       1000
  TCP winnuke                               enabled
  TCP SYN flood attack threshold            200
  TCP SYN flood alarm threshold             512
  TCP SYN flood source threshold            4000
  TCP SYN flood destination threshold       4000
```

```
TCP SYN flood timeout                    20
TCP SYN flood queue size                 1024
ICMP large packet                        enabled
```


Copyright © 2011, Juniper Networks, Inc.

show security screen statistics

Syntax

show security screen statistics
(zone *zone-name* | interface interface-name)
<node (*node-id* | all | local | primary)>

Release Information

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

Description

Display intrusion detection system (IDS) security screen statistics.

Options

none—Display IDS security for all zones and interfaces.

zone *zone-name* —(Optional) Display screen statistics for this security zone.

interface *interface-name*—(Optional) Display screen statistics for this interface.

node—(Optional) For chassis cluster configurations, display security screen statistics on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

Required Privilege Level

view

Related Documentation

- **clear security screen statistics on page 1080**
- **clear security screen statistics interface on page 1081**
- **clear security screen statistics zone on page 1082**

List of Sample Output

show security screen statistics zone scrzone on page 1555
show security screen statistics interface ge-0/0/3 on page 1556
show security screen statistics interface ge-0/0/1 node primary on page 1556

Output Fields

Table 159 on page 1553 lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Table 159: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.

Table 159: show security screen statistics Output Fields *(continued)*

Field Name	Field Description
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts
IP tear drop	Number of teardrop attacks. teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of Internet protocols (IP).
IP bad options	Number of invalid options.
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP security option	Number of IP security option attacks.

Copyright © 2011, Juniper Networks, Inc.

Table 159: show security screen statistics Output Fields *(continued)*

Field Name	Field Description
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK Proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, J Series and SRX Series devices running Junos OS rejects further connection requests from that IP address.
IP Block Fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.

show security screen statistics zone scrzone

```
user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                                Statistics
  ICMP flood                                   0
  UDP flood                                    0
  TCP winnuke                                  0
  TCP port scan                                91
  ICMP address sweep                           0
  TCP sweep                                    0
  UDP sweep                                    0
  IP tear drop                                 0
  TCP SYN flood                                0
  IP spoofing                                  0
  ICMP ping of death                           0
  IP source route option                       0
  TCP land attack                              0
  TCP SYN fragment                             0
  TCP no flag                                  0
```

```
  IP unknown protocol                       0
  IP bad options                            0
  IP record route option                    0
  IP timestamp option                       0
  IP security option                        0
  IP loose source route option              0
  IP strict source route option             0
  IP stream option                          0
  ICMP fragment                             0
  ICMP large packet                         0
  TCP SYN FIN                               0
  TCP FIN no ACK                            0
  Source session limit                      0
  TCP SYN-ACK-ACK proxy                     0
  IP block fragment                         0
  Destination session limit                 0
```

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type                             Statistics
  ICMP flood                                0
  UDP flood                                 0
  TCP winnuke                               0
  TCP port scan                             91
  ICMP address sweep                        0
  TCP sweep                                 0
  UDP sweep                                 0
  IP tear drop                              0
  TCP SYN flood                             0
  IP spoofing                               0
  ICMP ping of death                        0
  IP source route option                    0
  TCP land attack                           0
  TCP SYN fragment                          0
  TCP no flag                               0
  IP unknown protocol                       0
  IP bad options                            0
  IP record route option                    0
  IP timestamp option                       0
  IP security option                        0
  IP loose source route option              0
  IP strict source route option             0
  IP stream option                          0
  ICMP fragment                             0
  ICMP large packet                         0
  TCP SYN FIN                               0
  TCP FIN no ACK                            0
  Source session limit                      0
  TCP SYN-ACK-ACK proxy                     0
  IP block fragment                         0
  Destination session limit                 0
```

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
--------------------------------------------------------------------------
Screen statistics:
IDS attack type                             Statistics
  ICMP flood                                1
  UDP flood                                 1
  TCP winnuke                               1
  TCP port scan                             1
```


Copyright © 2011, Juniper Networks, Inc.

```
ICMP address sweep                        1
TCP sweep                                 1
UDP sweep                                 1
IP tear drop                              1
TCP SYN flood                             1
IP spoofing                               1
ICMP ping of death                        1
IP source route option                    1
TCP land attack                           1
TCP SYN fragment                          1
TCP no flag                               1
IP unknown protocol                       1
IP bad options                            1
IP record route option                    1
IP timestamp option                       1
IP security option                        1
IP loose source route option              1
IP strict source route option             1
IP stream option                          1
ICMP fragment                             1
ICMP large packet                         1
TCP SYN FIN                               1
TCP FIN no ACK                            1
Source session limit                      1
TCP SYN-ACK-ACK proxy                     1
IP block fragment                         1
Destination session limit                 1
```

show security softwires

Syntax show security softwires [softwire-name *softwire-name*]

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display a summary of information of all the softwire concentrators and details on concentrators with specified name.

Options softwire-name-str—Displays the softwire name.

Required Privilege Level view

Sample Output

```
user@host> show security softwires
Softwire Name            SC Address         Status   Number of SI connected
  SC-CSSI-1                 3001::1          Connected      2
  SC-CSSI-str00             3100::1          Active         0
  SC-CSSI-str01             3101::1          Inactive       0
  SC-CSSI-str02             3001::1          Connected      2520

user@host> show security softwires softwire-name SC-CSSI-1
Name of softwire: SC-CSSI-1
   SC status: Connected
   SC address: 3001::1
   Zone: trust
   VR ID: 0
 SI Address               SI Status                   SPU
 3001::2                  Active                      spu-1
 3001::2                  Active                      spu-21
 SI number: 2
0
```

 Copyright © 2011, Juniper Networks, Inc.

show security utm anti-spam statistics

Syntax show security utm anti-spam statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display antispam statistics for connections including total e-mail scanned, tagged and dropped connections.

Required Privilege Level view

Related Documentation

- **clear security utm anti-spam statistics on page 1083**
- **show security utm anti-spam status on page 1560**

Output Fields show security utm anti-spam statistics

Output fields are listed in the approximate order in which they appear.

show security utm anti-spam statistics

```
user@host> show security utm anti-spam statistics
Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

show security utm anti-spam status

Syntax show security utm anti-spam status

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display antispam status for connections including whitelist and blacklist server information.

Required Privilege Level view

Related Documentation

- **clear security utm anti-spam statistics on page 1083**
- **show security utm anti-spam statistics on page 1559**

Output Fields show security utm anti-spam status

Output fields are listed in the approximate order in which they appear.

show security utm anti-spam status

```
user@host> show security utm anti-spam status
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.juniper.net

DNS Server:
    Primary  :     1.2.3.4, Src Interface: ge-0/0/0
    Secondary:     0.0.0.0, Src Interface: ge-0/0/1
    Ternary  :     0.0.0.0, Src Interface: fe-0/0/2
```


Copyright © 2011, Juniper Networks, Inc.

show security utm anti-virus statistics

Syntax show security utm anti-virus statistics

Release Information Command introduced in Release 9.5 of Junos OS. Support for Sophos Antivirus added in Release 11.1 of Junos OS.

Description Display antivirus statistics for connections including clean and infected files and scan engine status.

Required Privilege Level view

Related Documentation

- **clear security utm antivirus statistics on page 1084**
- **show security utm anti-virus status on page 1562**
- **request security utm anti-virus juniper-express-engine on page 1117**
- **request security utm anti-virus kaspersky-lab-engine on page 1118**

Output Fields show security utm anti-virus statistics

Output fields are listed in the approximate order in which they appear.

show security utm anti-virus statistics

```
user@host>show security utm anti-virus statistics
Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 0
 Forwarded to scan engine:             0

Scan Mode:
     scan-all:                         0
     Scan-extension:                   0

 Scan Code:
     clear:                            0
     Infected:                         0
     Password files                    0
     Decompress layers:                0
     Corrupt files:                    0
     Out of resources:                 0
     Internal errors:                  0

 Fall back:           log-and-permit     block
     Engine not ready:            0               0
     Password file:               0               0
     Decompress layer:            0               0
     Corrupt files:               0               0
     Out of resources:            0               0
     Timeout:                     0               0
     Maximum content size:        0               0
     Too many requests:           0               0
     Others:                      0               0
```

show security utm anti-virus status

Syntax show security utm anti-virus status

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display antivirus status for connections including clean and infected files and scan engine status.

Required Privilege Level view

Related Documentation

- **clear security utm antivirus statistics on page 1084**
- **show security utm anti-virus statistics on page 1561**
- **request security utm anti-virus juniper-express-engine on page 1117**
- **request security utm anti-virus kaspersky-lab-engine on page 1118**

Output Fields show security utm anti-virus status

Output fields are listed in the approximate order in which they appear.

show security utm anti-virus status

```
user@host> show security utm anti-virus status
Anti-virus key expire date: 2010-07-30
    Update server: http://update.juniper-updates.net/EAV/SRX210/
           Interval: 1440 minutes
           Pattern update status: next update in 922 minutes
           Last result: download catalog file failed
    Anti-virus signature version: 000000_00
    Anti-virus signature compiler version: N/A
    Scan engine type: juniper-express-engine
    Scan engine information: Engine not ready
    Pattern type: N/A
    Total number of signatures: 11020
    New signatures (13):
    ------------------------
    00021301 Backdoor.Win32.Frauder.ky
    00021296 Rootkit.Win32.Pakes.e
    00021323 Trojan-Downloader.Win32.Exchanger.agf
    00021303 Trojan-Downloader.Win32.Injecter.arc
    00021325 Trojan-PSW.Win32.LdPinch.abgp
    00021299 Trojan-Ransom.Win32.Hexzone.pr
    00021298 Trojan-Spy.Win32.Zbot.fgt
    00021300 Trojan-Spy.Win32.Zbot.fgv
    00021324 Trojan-Spy.Win32.Zbot.fgw
    00021322 Trojan-Spy.Win32.Zbot.fhc
    00021321 Trojan-Spy.Win32.Zbot.fhd
    00021297 Trojan.Win32.FraudPack.aju
    00021302 Trojan.Win32.Inject.isz
    Modified signatures (0):
    ------------------------
    Removed signatures (1):
```

 Copyright © 2011, Juniper Networks, Inc.

```
------------------------
00020871 Trojan-GameThief.Win32.OnLineGames.bjpk
```

show security utm content-filtering statistics

Syntax show security utm content-filtering statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display content-filtering statistics for connections including lists of blocked files and the reasons for blocking.

Required Privilege Level view

Related Documentation

- **clear security utm content-filtering statistics on page 1085**

Output Fields show security utm content-filtering statistics

Output fields are listed in the approximate order in which they appear.

show security utm content-filtering statistics

```
user@host> show security utm content-filtering statistics
Content-filtering-statistic:         Blocked
     Base on command list:                    0
     Base on mime list:                       0
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
     EXE files:                               0
     ZIP files:                               0
     HTTP cookie:                             0
```


Copyright © 2011, Juniper Networks, Inc.

show security utm session

Syntax show security utm session

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display general UTM session information including all allocated sessions and active sessions.

Command introduced in Release 9.4 of Junos OS.

Required Privilege Level view

Related Documentation

- **clear security utm session on page 1086**
- **show security utm status on page 1566**

Output Fields show security utm session

Output fields are listed in the approximate order in which they appear.

show security utm session

```
user@host> show security utm session
Maximum sessions:           4000
 Total allocated sessions:         0
 Total freed sessions:             0
 Active sessions:                  0
```

show security utm status

Syntax show security utm status

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display whether the UTM service is running or not.

Required Privilege Level view

Related Documentation

- **clear security utm session on page 1086**
- **show security utm session on page 1565**

Output Fields show security utm status

Output fields are listed in the approximate order in which they appear.

show security utm status

```
user@host> show security utm status
UTM service status: Running
```


Copyright © 2011, Juniper Networks, Inc.

show security utm web-filtering statistics

Syntax show security utm web-filtering statistics

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display web-filtering statistics for connections including whitelist and blacklist hits and custom category hits.

Required Privilege Level view

Related Documentation

- **clear security utm web-filtering statistics on page 1087**
- **show security utm web-filtering status on page 1568**

Output Fields show security utm web-filtering statistics

Output fields are listed in the approximate order in which they appear.

show security utm web-filtering statistics

```
user@host> show security utm web-filtering statistics
Total requests:                 0
    white list hit:                 0
    Black list hit:                 0
    Queries to server:              0
    Server reply permit:            0
    Server reply block:             0
    Custom category permit:         0
    Custom category block:          0
    Cache hit permit:               0
    Cache hit block:                0
    Web-filtering sessions in total: 16000
    Web-filtering sessions in use:   0

Fall back:           log-and-permit      block
          Default                 0               0
          Timeout                 0               0

Connectivity               0               0

Too-many-requests          0               0
```

show security utm web-filtering status

Syntax show security utm web-filtering status

Release Information Command introduced in Release 9.5 of Junos OS.

Description Display whether the SurfControl CPA server is running or not.

Required Privilege Level view

Related Documentation

- **clear security utm web-filtering statistics on page 1087**
- **show security utm web-filtering statistics on page 1567**

Output Fields show security utm web-filtering status

Output fields are listed in the approximate order in which they appear.

show security utm web-filtering status

```
user@host> show security utm web-filtering status
UTM web-filtering status:
    Server status: SC-CPA server down
```


Copyright © 2011, Juniper Networks, Inc.

show security zones

Syntax

show security zones
<detail | terse>
< *zone-name* >

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display information about security zones.

Options

none—Display information about all zones.

detail | terse—(Optional) Display the specified level of output.

zone-name —(Optional) Display information about the specified zone.

Required Privilege Level

view

Related Documentation

- **security-zone on page 704**

List of Sample Output

show security zones on page 1569
show security zones abc on page 1570
show security zones abc detail on page 1570
show security zones terse on page 1570
show security zones my-shared-external on page 1570

Output Fields

Table 160 on page 1569 lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

Table 160: show security zones Output Fields

Field Name	Field Description
Security zone	Name of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.
Zone	Name of the zone.
Type	Type of the zone.

show security zones

```
user@host> show security zones
Functional zone: management
   Policy configurable: No
   Interfaces bound: 1
```

```
   Interfaces:
     ge-0/0/0.0
Security zone: Host
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     fxp0.0
Security zone: abc
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
Security zone: def
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/2.0
```

show security zones abc

```
user@host> show security zones abc
Security zone: abc
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

show security zones abc detail

```
user@host> show security zones abc detail
Security zone: abc
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

show security zones terse

```
user@host> show security zones terse
Zone                    Type
my-internal             Security
my-external             Security
dmz                     Security
my-shared-external      Security
```

show security zones my-shared-external

```
user@host> show security zones my-shared-external
Security zone: my-shared-external, Shared
  send reset for non SYN non session TCP packets : On
  IP/TCP reassembly for ALG on traffic from/to this zone: Yes
  Policy Configurable: Yes
  Interfaces bound:1.
    ge-0/1/1.0
    IP classification: Disabled.
```


Copyright © 2011, Juniper Networks, Inc.

show security zones type

Syntax

show security zones type
(functional | security)
<detail | terse>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display information about security zones of the specified type.

Options

functional—Display functional zones.

security—Display security zones.

detail | terse—(Optional) Display the specified level of output.

Required Privilege Level

view

Related Documentation

- **security-zone on page 704**

List of Sample Output

show security zones type functional on page 1571
show security zones type security on page 1572
show security zones type security terse on page 1572
show security zones type security detail on page 1572

Output Fields

Table 161 on page 1571 lists the output fields for the **show security zones type** command. Output fields are listed in the approximate order in which they appear.

Table 161: show security zones type Output Fields

Field Name	Field Description
Security zone	Zone name.
Policy configurable	Whether the policy can be configured or not.
Interfaces	List of the interfaces in the zone.
Interfaces bound	Number of interfaces in the zone.
Zone	Name of the zone.
Type	Type of the zone.

show security zones type functional

```
user@host> show security zones type functional
Security zone: Host
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
```

```
fxp0.0
Security zone: fz
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
ge-0/0/1.0
```

show security zones type security

```
user@host> show security zones type security
Security zone: Host
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
fxp0.0
Security zone: fz
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:
ge-0/0/1.0
```

show security zones type security terse

```
user@host> show security zones type security terse
Zone                    Type
my-internal             Security
my-external             Security
dmz                     Security
my-shared-external      Security
```

show security zones type security detail

```
user@host> show security zones type security detail
Security zone: HOST
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: all
  Interfaces:
```


Copyright © 2011, Juniper Networks, Inc.

show services accounting

Syntax

show services accounting
aggregation
errors
flow
flow-detail
memory
packet-size-distribution
status
usage

Release Information

Command introduced in Release 10.4 of Junos OS.

Description

Display sampled accounting service.

Options

aggregation—Display aggregation information.

errors—Display error statistics.

flow—Display flow information.

flow-detail—Display flow detail.

memory—Display memory information.

packet-size-distribution—Display packet size distribution.

status—Display service accounting parameters.

usage—Display CPU usage.

Required Privilege Level

view

Copyright © 2011, Juniper Networks, Inc.

show services accounting aggregation

Syntax show services accounting aggregation

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display aggregation information for the accounting service.

Options as—Display aggregation type AS.

destination-prefix—Display aggregation type destination-prefix.

protocol-port—Display aggregation type protocol-port.

source-destination-prefix—Display aggregation type source-destination-prefix.

source-prefix—Display aggregation type source-prefix.

template—Display aggregation type template.

Required Privilege Level view

Copyright © 2011, Juniper Networks, Inc.

show services accounting aggregation template

Syntax show services accounting aggregation template

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display aggregation type template.

Options detail—Display detailed output.

extensive—Display extensive output.

template-name—Display name of the template.

terse—Display terse output (default).

Required Privilege Level view

Copyright © 2011, Juniper Networks, Inc.

show services accounting flow-detail

Syntax show services accounting flow-detail

Release Information Command introduced in Release 10.4 of Junos OS.

Description Display flow detail

Options

destination-as—Filter term destination AS.

destination-port—Filter term destination port.

destination-prefix—Filter term destination prefix.

detail—Display detailed output.

extensive—Display extensive output.

input-snmp-interface-index—Filter term input SNMP interface index.

limit—Display maximum number of flows to display.

name—Display name of the service, wildcard, or 'all'.

order—Display order for displaying flows.

output-snmp-interface-index—Filter term output SNMP interface index.

proto—Filter term protocol.

source-as—Filter term source AS.

source-port—Filter term source port.

source-prefix—Filter term source prefix.

terse—Display terse output (default).

tos—Filter term ToS.

Required Privilege Level view

Copyright © 2011, Juniper Networks, Inc.

show services application-identification application-system-cache

Syntax show services application-identification application-system-cache

Release Information Command introduced in Release 10.2 of Junos OS.
Command updated in Release 10.4 of Junos OS.

Description Display application ID from default port/protocol binding or from the application system cache.

Required Privilege Level view

Related Documentation
- Table 162 on page 1577
- **clear services application-identification application-system-cache on page 1088**

List of Sample Output **show services application-identification application-system-cache on page 1577**

Output Fields Table 162 on page 1577 lists the output fields for the **show services application-identification application-system-cache** command. Output fields are listed in the approximate order in which they appear.

Table 162: show services application-identification application-system-cache Output Fields

Field Name	Field Description
application-cache	On or Off status of the application cache.
nested-application-cache	On or Off status of the nested application cache.
cache-entry-timeout	The number of seconds the mapping information is saved.
pic	The PIC location of the cache.
Vsys-ID	Application identification number.
IP address	IP address.
Port	Port number that is used with the current session.
Protocol	Name of the session protocol.
Application	Name of the service and application that was identified.

show services application-identification application-system-cache

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
  nested-application-cache: on
  cache-entry-timeout: 3600 seconds
  pic: 2/0
```

```
Vsys-ID     IP address        Port     Protocol     Application
  0           5.0.0.1           80       TCP          HTTP

  0           7.0.0.1           80       TCP          HTTP:FACEBOOK
```


Copyright © 2011, Juniper Networks, Inc.

show services application-identification counter

Syntax show services application-identification counter

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the status of all Junos OS application identification per SPU counter values.

Required Privilege Level view

Related Documentation
- **clear services application-identification counter on page 1089**

List of Sample Output **show services application-identification counter on page 1580**

Output Fields Table 163 on page 1579 lists the output fields for the **show services application-identification counter** command. Output fields are listed in an approximate order in which they appear.

Table 163: show services application-identification counter Output Fields

Field Name	Field Description
AI cache hits	Number of sessions found application in AI cache.
AI cache hits by nested application	Number of sessions found nested application in AI cache.
AI cache misses	Number of sessions those did not find application from AI cache.
AI matches	Number of times an application is successfully identified.
AI no-matches	Number of times no application match is found.
AI partial matches	Number of times an application matched only one side signature.
AI no-partial matches	Number of times no partial match occurs.
Sessions that triggered Appid create session API	Number of sessions that carried out the internal session create process.
Sessions that do not incur signature match or decoding	Number of sessions that do not receive heavy weighted application identification process.
Sessions that incur signature match or decoding	Number of sessions that receive heavy weighted application identification process.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server layer-7 bytes processed	Number of client-to-sever Layer 7 payload bytes processed.

Copyright © 2011, Juniper Networks, Inc.

Table 163: show services application-identification counter Output Fields *(continued)*

Field Name	Field Description
Server-to-client layer-7 bytes processed	Number of server-to-client Layer 7 payload bytes processed.
Terminal first data packets on both direction	Number of times the first data packet on each direction triggers final application match.
Unspecified encrypted sessions	Number of encrypted sessions identified by heuristics.
Encrypted P2P sessions	Number of encrypted P2P sessions identified by heuristics.

show services application-identification counter

```
user@host> show services application-identification counter
pic: 1/0
  Counter type                                                    Value
 AI cache hits                                                        0
 AI cache hits by nested application                                  0
 AI cache misses                                                      0
 AI matches                                                           0
 AI no-matches                                                        0
 AI partial matches                                                   0
 AI no-partial matches                                                0
 Sessions that triggered Appid create session API                     0
 Sessions that do not incur signature match or decoding               0
 Sessions that incur signature match or decoding                      0
 Client-to-server packets processed                                   0
 Server-to-client packets processed                                   0
 Client-to-server layer-7 bytes processed                             0
 Server-to-client layer-7 bytes processed                             0
 Terminal first data packets on both direction                        0
 Unspecified encrypted sessions                                       0
 Encrypted P2P sessions                                               0
```


Copyright © 2011, Juniper Networks, Inc.

show services application-identification version

Syntax show services application-identification version

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the Junos OS application package version.

Required Privilege Level view

Related Documentation

- **request services application-identification download on page 1092**

List of Sample Output **show services application-identification version on page 1581**

show services application-identification version The following output shows that the application package version is 1608.

```
user@host> show services application-identification version
Application package version: 1608
```

show services unified-access-control authentication-table

Syntax show services unified-access-control authentication-table

Release Information Command introduced in Release 9.4 of Junos OS.

Description Display a summary of the authentication table entries configured from the Infranet Controller. Authentication tables store mappings between traffic sessions and Unified Access Control (UAC) roles. The Infranet Controller uses the roles specified in the mappings to help determine which UAC policies to apply to a session.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options **detail**—Display a detailed view of all authentication table entries.

identifier *id*—Display information about a specific authentication table entry by identification number.

Required Privilege Level view

List of Sample Output

show services unified-access-control authentication-table on page 1582
show services unified-access-control authentication-table detail on page 1582
show services unified-access-control authentication-table identifier 1 on page 1582

show services unified-access-control authentication-table

```
user@host> show services unified-access-control authentication-table
Id    Source IP       Username     Age      Role identifier
1     172.24.72.79    atsang       0        0000000001.000005.0
```

show services unified-access-control authentication-table detail

```
user@host> show services unified-access-control authentication-table detail
Identifier: 1
  Source IP: 172.24.72.79
  Username: atsang
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 Personal Firewall
    1183670148.427197.0 UAC
```

show services unified-access-control authentication-table identifier 1

```
user@host> show services unified-access-control authentication-table identifier 1
Identifier: 1
  Source IP: 172.24.72.79
  Username: atsang
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 Personal Firewall
    1183670148.427197.0 UAC
```


Copyright © 2011, Juniper Networks, Inc.

show services unified-access-control policies

Syntax show services unified-access-control policies

Release Information Command introduced in Release 9.4 of Junos OS.

Description Display a summary of resource access policies configured from the Infranet Controller.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options **detail**—Display a detailed view of all policies.

identifier *id*—Display information about a specific policy by identification number.

Required Privilege Level view

List of Sample Output

show services unified-access-control policies on page 1583
show services unified-access-control policies detail on page 1583
show services unified-access-control policies identifier 1 on page 1583

show services unified-access-control policies

```
user@host> services unified-access-control policies
Id    Resource                Action Apply        Role identifier
1     10.100.15.0/24:*        allow  selected     1113249951.100616.0
2     10.100.17.0/24:*        deny   all
```

show services unified-access-control policies detail

```
user@host> services unified-access-control policies detail
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
    1112927873.881659.0 Antivirus
    1183670148.427197.0 UAC
Identifier: 2
  Resource: 10.100.17.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Resource: 10.100.18.0/24:*
  Action: deny
  Apply: all
```

show services unified-access-control policies identifier 1

```
user@host> show services unified-access-control policies identifier 1
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
```

```
1112927873.881659.0 Antivirus
1183670148.427197.0 UAC
```


Copyright © 2011, Juniper Networks, Inc.

show services unified-access-control status

Syntax show services unified-access-control status

Release Information Command introduced in Release 9.4 of Junos OS.

Description Display the status of the connection between the SRX Series device and the Infranet Controller as well as statistics to help debug connections to the Infranet Controller.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Required Privilege Level view

List of Sample Output show services unified-access-control status on page 1585

show services unified-access-control status

```
user@host> show services unified-access-control status
Host           Address         Port   Interface     State
dev106vm26     10.64.11.106    11123  ge-0/0/0.0    connected
dev107vm26     10.64.11.106    11123  ge-0/0/0.0    closed
```

Copyright © 2011, Juniper Networks, Inc.

show system services dhcp client

Syntax

show system services dhcp client
< *interface-name* >
<statistics>

Release Information

Command introduced in Release 8.5 of Junos OS.

Description

Display information about DHCP clients.

Options

none—Display DHCP information for all interfaces.

interface-name —(Optional) Display DHCP information for the specified interface.

statistics—(Optional) Display DHCP client statistics.

Required Privilege Level

view and system

Related Documentation

- **dhcp on page 162**
- **request system services dhcp on page 1122**

List of Sample Output

show system services dhcp client on page 1587
show system services dhcp client ge-0/0/1.0 on page 1587
show system services dhcp client statistics on page 1588

Output Fields

Table 164 on page 1586 lists the output fields for the **show system services dhcp client** command. Output fields are listed in the approximate order in which they appear.

Table 164: show system services dhcp client Output Fields

Field Name	Field Description
Logical Interface Name	Name of the logical interface.
Client Status	State of the client binding.
Vendor Identifier	Vendor ID.
Server Address	IP address of the DHCP server.
Address obtained	IP address obtained from the DHCP server.
Lease Obtained at	Date and time the lease was obtained.
Lease Expires at	Date and time the lease expires.
DHCP Options	• **Name: server-identifier**, **Value:**IP address of the name server. • **Name: device**, **Value:** IP address of the name device. • **Name: domain-name**, **Value:** Name of the domain.

Copyright © 2011, Juniper Networks, Inc.

Table 164: show system services dhcp client Output Fields *(continued)*

Field Name	Field Description
Packets dropped	**Total** packets dropped.
Messages received	**Number of the following DHCP messages received:** • **DHCPOFFER**—First packet received on a logical interface when DHCP is enabled. • **DHCPACK**—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stop the earlier timer added for DHCPACK. • **DHCPNAK**—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.
Messages sent	**Number of the following DHCP messages sent:** • **DHCPDECLINE**—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet. • **DHCPDISCOVER**—Packet sent on the interface for which the DHCP client is enabled. • **DHCPREQUEST**—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer. • **DHCPINFORM**—Packet sent to the DHCP server for local configuration parameters. • **DHCPRELEASE**—Packet sent to the DHCP server to relinquish network address and cancel remaining lease. • **DHCPRENEW**—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server. • **DHCPREBIND**—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.

show system services dhcp client

```
user@host> show system services dhcp client
Logical Interface Name       ge-0/0/1.0
      Hardware address        00:0a:12:00:12:12
      Client Status           bound
      Vendor Identifier       ether
      Server Address          10.1.1.1
      Address obtained        10.1.1.89
      update server           enabled
      Lease Obtained at       2006-08-24 18:13:04 PST
      Lease Expires at        2006-08-25 18:13:04 PST
 DHCP Options :
           Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
           Name: server-identifier, Value: 10.1.1.1
           Name: router, Value: [ 10.1.1.80 ]
           Name: domain-name, Value: netscreen-50
```

show system services dhcp client ge-0/0/1.0

```
user@host>  show system services dhcp client ge-0/0/1.0
Logical Interface name         ge-0/0/1.0
Hardware address        00:12:1e:a9:7b:81
Client status           bound
Address obtained        30.1.1.20
Update server           disabled
Lease obtained at       2007-05-10 18:16:18 UTC
Lease expires at        2007-05-11 18:16:18 UTC
DHCP options:
```

```
    Name: server-identifier, Value: 30.1.1.2
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
Name: domain-name, Value: englab.juniper.net
```

show system services dhcp client statistics

```
user@host> show system services dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    DHCPOFFER                 0
    DHCPACK                   8
    DHCPNAK                   0
Messages sent:
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               1
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 7
    DHCPREBIND                0
```


Copyright © 2011, Juniper Networks, Inc.

show system services dhcp relay-statistics

Syntax **show system services dhcp relay-statistics**

Release Information Command introduced in Release 8.5 of Junos OS.

Description Display information about the DHCP relay.

Required Privilege Level view and system

Related Documentation
- **dhcp on page 162**

List of Sample Output **show system services dhcp relay-statistics on page 1589**

Output Fields Table 165 on page 1589 lists the output fields for the **show system services dhcp relay-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 165: show system services dhcp relay-statistics Output Fields

Field Name	Field Description
Received packets	Total DHCP packets received.
Forwarded packets	Total DHCP packet forwarded.
Dropped packets	Total DHCP packets dropped for the following reasons: • **Due to a missing interface in the relay database**—Number of packets discarded because they did not belong to a configured interface. • **Due to a missing matching routing instance**—Number of packets discarded because they did not belong to a configured routing instance. • **Due to an error during packet read**—Number of packets discarded because of a system read error. • **Due to an error during packet send**—Number of packets that the DHCP relay application could not send. • **Due to an invalid server address**—Number of packets discarded because an invalid server address was specified. • **Due to a missing valid local address**—Number of packets discarded because there was no valid local address. • **Due to a missing route to the server or client**—Number of packets discarded because there were no addresses available for assignment.

show system services dhcp relay-statistics

```
user@host> show system services dhcp relay-statistics
  Received packets: 4
  Forwarded packets: 4
  Dropped packets: 4
    Due to missing interface in relay database: 4
    Due to missing matching routing instance: 0
    Due to an error during packet read: 0
    Due to an error during packet send: 0
```

```
Due to invalid server address: 0
Due to missing valid local address: 0
Due to missing route to server/client: 0
```


Copyright © 2011, Juniper Networks, Inc.

show system snapshot media

Syntax show system snapshot media *media-type*

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the snapshot information for both root partitions on SRX Series devices

Options

- internal— Show snapshot information from internal media.
- usb— Show snapshot information from device connected to USB port.
- external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.

Required Privilege Level View

show system snapshot media internal

show system snapshot media internal

```
Information for snapshot on       internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos  : 10.1B3-domestic
Information for snapshot on       internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos  : 10.2-20100112.0-domestic
```

show system snapshot media usb

show system snapshot media usb

```
Information for snapshot on       usb (/dev/da1s1a) (primary)
            Creation date: Jul 24 16:16:01 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090723_1017-domestic
            Information for snapshot on       usb (/dev/da1s2a) (backup)
            Creation date: Jul 24 16:17:13 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090724_0719-domestic
```

Copyright © 2011, Juniper Networks, Inc.

show system storage partitions

Syntax show system storage partitions

Release Information Command introduced in Release 10.2 of Junos OS.

Description Displays the partitioning scheme details on SRX Series devices.

Required Privilege Level View

show system storage partitions (dual root partitioning)

show system storage partitions

```
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   altroot
      s2a    293M   /
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

show system storage partitions (single root partitioning)

show system storage partitions

```
Boot Media: internal (da0)
Partitions Information:
  Partition  Size   Mountpoint
      s1a    898M   /
      s1e    24M    /config
      s1f    61M    /var
```

show system storage partitions (USB)

show system storage partitions

```
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   /
      s2a    293M   altroot
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```


Copyright © 2011, Juniper Networks, Inc.

show wan-acceleration status

Syntax **show wan-acceleration status**

Release Information Command introduced in Release 8.5 of Junos OS.

Description Display the redirection status and related information about the WXC Integrated Services Module (ISM 200) for WAN acceleration.

Required Privilege Level view

Related Documentation
- **request wan-acceleration login on page 1129**

List of Sample Output **show wan-acceleration status on page 1593**

Output Fields Table 166 on page 1593 lists the output fields for the **show wan-acceleration status** command. Output fields are listed in the approximate order in which they appear.

Table 166: show wan-acceleration status Output Fields

Field Name	Field Description
Redirection status	Indicates whether traffic redirection to the WXC ISM 200 is active.
Interface	Name of the WXC ISM 200 interface.
Primary address	Address used to manage the WXC ISM 200, and as the source address of traffic sent across the WAN.
Secondary address	Source address of traffic destined for an alternate WAN path when the Multi-Path feature is configured (optional).
JUNOS version	Installed version of Junos OS.
WXOS version	Installed version of WXOS.
JUNOS/WXOS protocol	Indicates whether the Junos OS and WXOS versions are compatible.

show wan-acceleration status

```
user@host> show wan-acceleration status
Redirection status: active, Interface: wx-2/0/0
Primary address: 10.87.5.2, Secondary address: 0.0.0.0
JUNOS version: 9.0R1 Enhanced Services
WXOS version: 5.4.6.0j
JUNOS/WXOS protocol: Version compatible
```

show wlan access-points

Syntax show wlan access-points <*name*> <detail> <virtual-access-points> <client-associations> <neighbors>

Release Information Command introduced in Release 10.0 of Junos OS.

Description Display access point status information.

Options none—Display the status of all access points on the services gateway.

name—(Optional) Display information about a specific access point on the services gateway.

detail—(Optional) Display detailed information about a specific access point on the services gateway.

virtual-access-points—(Optional) Display information about the virtual access points configured on a specific access point on the services gateway.

client-associations—(Optional) Display information about the client associations on a specific access point on the services gateway.

neighbors—(Optional) Display information about the neighbor access points of a specific access point on the services gateway.

Required Privilege Level view

Output Fields Table 167 on page 1594 lists the output fields for the **show wlan access-points** command. Output fields are listed in the approximate order in which they appear.

Table 167: show wlan access-points Output Fields

Field Name	Field Description
Access-Point	Name of the access point.
Type	Access point type, for example “Ext” for external access point.
Interface	PoE interface on the SRX Series device to which the access point is connected.
Radio-mode/Channel	Physical Layer (PHY) standard mode of the radio and the channel used for transmitting and receiving.

show wlan access-points

```
user@host> show wlan access-points
Active access points information
Access-Point  Type  Interface  Radio-mode/Channel
wap-1         Ext   ge-1/0/2   bgn/2, an/157
wap-2         Ext   ge-2/0/4   bg/5, bg/145
wap-3         Ext   ge-1/0/6   an/145, an/157
ap001f12e088c0 Ext fe-0/0/4.0 an/108, bgn/7
```


Copyright © 2011, Juniper Networks, Inc.

show wlan access-points wap-3

```
user@host> show wlan access-points wap-3
Active access point information
Access Point        : wap-3
Type                : External
Access Interface    : ge-2/0/4
IPv4 Address        : 10.210.5.7
Packet Capture      : disabled
Radio1              : Mode: None, Channel: None
Radio2              : Mode: bg, Channel: 5
```

show wlan access-points ap001f12e088c0 detail

```
user@host> show wlan access-points ap001f12e088c0 detail
Active access point detail information

Access Point        : ap001f12e088c0
Type                : External
Location            : Default Location
Serial Number       : 850001811
Firmware Version    : 10.1.0.1
Access Interface    : vlan.0
Packet Capture      : Disabled
Ethernet Port:
    MAC Address     : 00:1F:12:E0:88:C0
    IPv4 Address    : 16.1.1.2
Radio1:
    Status          : On
    MAC Address     : 00:1F:12:E0:88:C0
    Mode            : IEEE 802.11a/n
    Channel         : 36 (5180 MHz)
Radio2:
    Status          : On
    MAC Address     : 00:1F:12:E0:88:D0
    Mode            : IEEE 802.11b/g/n
    Channel         : 6 (2437 MHz)
```

show wlan access-points wap-3 virtual-access-points

```
user@host> show wlan access-points wap-3 virtual-access-points
Virtual access points information

Access Point: wap-3
Radio1:
   VAP0:
      SSID                 : juniper_ap_0
      MAC Address          : 00:11:22:33:44:55
      VLAN ID              : 5
      Traffic Statistics:
        Input Bytes        : 37979930
        Output Bytes       : 54231321
        Input Packets      : 210737
        Output Packets     : 298451
   VAP3:
      SSID                 : juniper_ap_3
      MAC Address          : 00:11:22:33:44:58
      VLAN ID              : 15
      Traffic Statistics:
        Input Bytes        : 83421130
        Output Bytes       : 21221311
        Input Packets      : 510837
        Output Packets     : 238451
Radio2:
   VAP0:
```

```
      SSID                 : juniper_ap_7
      MAC Address          : 00:11:22:33:44:75
      VLAN ID              : 5
      Traffic Statistics:
        Input Bytes        : 67079335
        Output Bytes       : 34932321
        Input Packets      : 415737
        Output Packets     : 308451
   VAP3:
      SSID                 : juniper_ap_3
      MAC Address          : 00:11:22:33:44:78
      VLAN ID              : 49
      Traffic Statistics:
        Input Bytes        : 37979930
        Output Bytes       : 54231321
        Input Packets      : 512837
        Output Packets     : 901151
```

show wlan access-points wap-3 client-associations

```
user@host> show wlan access-points wap-3 client-associations
Access point client associations information

Access point: wap-3

VAP          Client MAC Address  Auth  Packets Rx/Tx  Bytes Rx/Tx
Radio0:VAP0  00:44:11:22:33:77    OK   4132/55123     925568/6835252
Radio0:VAP0  00:74:f1:e2:13:8a    OK   132/8133       925568/6835252
Radio1:VAP0  00:8a:fe:92:83:9c    OK   5/203          524/22736
Radio1:VAP0  00:3b:f7:c3:4e:6b    OK   76/623         /6835252
```

show wlan access-points wap-3 neighbors

```
user@host> show wlan access-points wap-3 neighbors
Access point neighbors information

Access point: wap-3

MAC                Privacy  WPA  Band  Channel  SSID
00:11:22:33:44:55  Off      Off  2.4   10       xyz-ap
00:12:23:45:56:67  On       On   5     100      abc-ap
```


Copyright © 2011, Juniper Networks, Inc.

show wlan diagnostics

Syntax show wlan diagnostics

Release Information Command introduced in Release 10.2 of Junos OS.

Description Display the Wireless LAN diagnostics information status such as Packet Capture and System log messages.

Required Privilege Level maintenance

Example **user@host# show wlan diagnostics**

Example

```
Active access points diagnostics information

    Access-Point        Pcap-Status   Pcap-Interface   Syslog-Status
    mav0                Off           None             Off
    mav1                Off           None             Off
```

Copyright © 2011, Juniper Networks, Inc.

PART 3

Index

- Index on page 1601

Copyright © 2011, Juniper Networks, Inc.

Index

Symbols

#, comments in configuration statements....xlii
( ), in syntax descriptions....xlii
(antivirus utm-policy)....489
(content-filtering utm-policy)....466
< >, in syntax descriptions....xli
[ ], in configuration statements....xlii
{ }, in configuration statements....xlii
| (pipe), in syntax descriptions....xlii

A

Access Configuration Statement Hierarchy....3
access-point statement
    WLAN....950
access-point-name statement....156
access-point-options statement
    WLAN....954
access-point-queues statement
    WLAN....955
access-profile statement
    (Dynamic VPNs)....309
    (IPsec VPNs)....309
Accounting-Options Configuration Statement Hierarchy....53
ack-number statement....310
action (web filtering)....313
action statement....311, 312
activation-priority statement....156
active-policy statement....313
adaptive-shaper statement....106
adaptive-shapers statement....107
address statement....545, 645, 859, 899
    (ARP Proxy Services Gateway)....315
    (Destination NAT Services Gateway)....315
    (IKE Gateway)....316
    (Zone Address Book)....317
address-assignment statement....8
address-blacklist....318
address-book statement....318
address-mapping statement....319
address-persistent statement....319
address-pool statement....10
address-set statement....320
address-whitelist....320
admin-email....321
admin-search statement....11
administrator statement....321
administrator-email....322
administrator-email (fallback-block)....330, 415
aging statement....323
alarm-threshold statement....323
alarm-without-drop statement....324
alert statement....324
alg statement....57, 325
algorithm statement....329
all-day statement....258
all-tcp statement....329
allow-dns-reply statement....330
allow-email (virus-detect)....331
allow-icmp-without-flow statement....331
always-send statement....331
analysis no-reports statement....332
annex....157
anomaly statement....332
antispam (feature-profile)....333
antispam (utm-policy)....334
antivirus (feature-profile)....335
antivirus (utm-policy)....337
apn (gtp)....338
application AppDDoS....339
application identification
    services....861
application identification services
    nested application settings....875
application statement
    (application identification)....860, 874
    (Protocol Binding Custom Attack)....339
    (Security Policies)....340
application-firewall....341
application-identification statement....342
application-level DDoS rule statement....680

application-protocol statement....58
application-screen statement
(H323)....343
(MGCP)....343
(SCCP)....344
(SIP)....345
application-services....347
application-services statement....348
application-services statement (Application Firewall)....346
application-services statement (Unified Access Control)....348
application-system-cache statement....349
application-system-cache-timeout statement....349
Applications Configurations Statement Hierarchy....55
arbitration-inter-frame-space statement
WLAN....956
asap statement....424
assemble statement statement....11
associate-timeout statement....350, 645, 702
attack-threshold statement....351
attack-type statement
(Custom Attack)....352, 353, 354
attacks statement
(Exempt Rulebase)....351
(IPS Rulebase)....352
authentication statement....357
authentication-algorithm statement....358
authentication-method statement....157, 359
authentication-order statement 12
authorization statement....895
auto-re-enrollment statement....360
automatic statement....360

B

BA classifier....108
background-queue statement
WLAN....956
bandwidth (radio-router)....158
banner statement
(FTP, HTTP, Telnet)....12
(Web authentication)....13
base-distinguished-name statement....14
beacon-interval statement
WLAN....957
bearer-bandwidth-limit statement....158
best-effort-queue statement
WLAN....957
bind-interface statement....361
block-command....361
block-content-type....362
block-mime....362
braces, in configuration statements....xlii
brackets
angle, in syntax descriptions....xli
square, in configuration statements....xlii
bridge domain
routing interface....72
VLAN identifier....73
VLAN identifier list....74
bridge statement....363
Bridge-Domains Configuration Statement Hierarchy....69
bridge-domains statement....70
bridge-options statement....71
broadcast-multicast-rate-limit statement
WLAN....958
bundle statement....159

C

c-timeout statement....364
ca-identity statement....364
ca-profile statement....365, 862
ca-profile-name statement....366
cache....366
cache-size statement....367
call-flood statement....367
captive-portal statement....863
captive-portal statement (Unified Access Control policy)....864
category (web filtering)....369
category statement....368
(Security Logging)....368
cellular-options statement....160
certificate statement....369
certificate-id statement....370
chain statement....371
challenge-password statement....372
channel statement
WLAN....958
Chassis Configuration Statement Hierarchy....75
chassis-cluster statement....810
class name....112
Class-of-Service Configuration Statement Hierarchy....103

Copyright © 2011, Juniper Networks, Inc.

classifiers (Cos).....108
clear chassis cluster control-plane statistics command.....1002
clear chassis cluster data-plane statistics command.....1003
clear chassis cluster failover-count command.....1004
clear chassis cluster ip-monitoring failure-count.....1006
clear chassis cluster ip-monitoring failure-count ip-address.....1007
clear chassis cluster statistics command.....1008
clear dhcpv6 server binding command.....1009
clear dhcpv6 server statistics command.....1010
clear esis adjacency command.....1011
clear esis statistics command.....1012
clear gtp tunnels command.....1013
clear interfaces statistics swfabx command.....1014
clear lacp statistics interfaces command.....1015
clear network-access requests pending command.....1016
clear network-access requests statistics command.....1017
clear network-access securid-node-secret-file command.....1018
clear security alg h323 counters command.....1019
clear security alg ike-esp-nat command.....1020
clear security alg mgcp calls command.....1021
clear security alg mgcp counters command.....1022
clear security alg sccp calls command.....1023
clear security alg sccp counters command.....1024
clear security alg sip calls command.....1025
clear security alg sip counters command.....1026
clear security application-firewall rule-set statistics.....1027
clear security datapath-debug counters command.....1028
clear security dynamic-vpn all command.....1029
clear security dynamic-vpn user command.....1030
clear security firewall-authentication history address command.....1032
clear security firewall-authentication history command.....1031
clear security firewall-authentication history identifier command.....1033
clear security firewall-authentication users address command.....1035
clear security firewall-authentication users command.....1034
clear security firewall-authentication users identifier command.....1036
clear security flow ip-action family command.....1037
clear security flow session all command.....1038
clear security flow session application command.....1039
clear security flow session destination-port command.....1041
clear security flow session destination-prefix command.....1042
clear security flow session family 1044
clear security flow session interface command.....1045
clear security flow session protocol command.....1046
clear security flow session resource-manager command.....1048
clear security flow session session-identifier command.....1049
clear security flow session source-port command.....1050
clear security flow session source-prefix command.....1051
clear security gprs sctp counters command.....1052
clear security group-vpn member ike security-associations command.....1053
clear security group-vpn member ipsec security-assocations command.....1054
clear security group-vpn member kek security-assocations command.....1055
clear security group-vpn server command.....1056
clear security idp 1057
clear security idp application-identification application-system-cache command.....1058
clear security idp attack table command.....1059
clear security idp counters application-identification command.....1060
clear security idp counters dfa command.....1061
clear security idp counters flow command.....1062
clear security idp counters ips command.....1063
clear security idp counters log command.....1064
clear security idp counters packet command.....1065
clear security idp counters policy-manager command.....1066
clear security idp counters tcp-reassembler command.....1067
clear security idp ssl-inspection session-id-cache command.....1068

clear security ike respond-bad-spi-count command....1069
clear security ike security-associations command....1070
clear security ipsec security-associations command....1072
clear security ipsec statistics command....1074
clear security nat incoming-table command....1075
clear security nat source persistent-nat-table command....1076
clear security pki key-pair command....1077
clear security pki local-certificate command....1078
clear security policies statistics command....1079
clear security screen statistics command....1080
clear security screen statistics interface command....1081
clear security screen statistics zone command....1082
clear security utm anti-spam statistics....1083
clear security utm antivirus statistics....1084
clear security utm content-filtering statistics....1085
clear security utm session....1086
clear security utm web-filtering statistics....1087
clear services application-identification application-system-cache command....1088
clear services application-identification counter command....1089
clear-threshold statement....372
client-group statement....15
client-identifier statement....160
client-idle-timeout statement....15
client-list-name statement....896
client-name-filter statement....16
client-session-timeout statement....16
clients statement....373
cluster statement....79
    channel-management....959
    default-cluster....965
    interfaces....971
    name....975
    WLAN....960, 963, 971
co-location statement
    security....373
code statement....374
code-point statement....109
comments, in configuration statements....xlii
compression-device statement....161
condition statement....204
configuration statement....552, 702, 810
configuration-file statement....17
connection-flood statement....374
connection-rate-threshold statement....375
connections-limit statement....375
console statement
    WLAN....963
container statement....376
content-filtering....377
content-filtering (utm-policy)....378
content-size....379
content-size-limit....380
context statement....380, 381
control-link-recovery statement....80
control-ports statement....81
conventions
    notice icons....xl
    text and syntax....xli
corrupt-file....381
count statement....17
    (Custom Attack)....382
    (Security Policies)....382
country statement
    WLAN....964
credit (radio-router)....161
crl statement....383
curly braces, in configuration statements....xlii
custom-attack statement....384
custom-attack-group statement....388
custom-attacks statement....388
custom-block-message....389
custom-message (antivirus notification-options fallback-block/non-block)....389
custom-message (antivirus pattern-update email-notify)....391
custom-message-subject (antivirus notification-options fallback-block/non-block)....390
custom-message-subject (antivirus notification-options virus-detection)....391
custom-objects....392
custom-tag-string....392
custom-url-category....393
customer support....xlii
    contacting JTAC....xlii

D

daily statement....259
data-length statement....393
ddp-segment statement....424

Copyright © 2011, Juniper Networks, Inc.

ddp-stream statement....424
dead-peer-detection statement....395
decoding-error statement....552
decompress-layer....395
decompress-layer-limit....396
default (antivirus fallback-options)....396
default (web-filtering fallback-settings)....397
default statement....109
default-policy statement....397
default-profile statement....18
deny statement
(Policy)....398
(SIP)....399
description statement
(IDP Policy)....399
(Security Policies)....400
destination statement
(Destination NAT Services Gateway)....401
(IP Headers in Signature Attack)....402
destination-address statement
(Destination NAT Services Gateway)....403
(IDP Policy)....403
(Security Policies Flag)....405
(Security Policies)....404
(Source NAT Services Gateway)....406
destination-except statement....407
destination-ip statement....407
destination-ip-based statement....408
destination-nat statement
(Destination NAT Services Gateway)....408
destination-port statement....59
(Destination NAT Services Gateway)....409
(Signature Attack)....409
destination-threshold statement....410
detect-shellcode statement....410
detector statement....411
df-bit statement....411
dh-group statement....412
dhcp statement....162
dhcp-attributes statement IPv4....19
dhcp-attributes statement IPv6....20
dhcp-local-server....916
dhcpv6....914
direction statement
(Custom Attack)....413
(Dynamic Attack Group)....414
disable statement....196
ES-IS....229, 231
disable-call-id-hiding statement....414
disable-dot11d statement
WLAN....966
display-host (virus-detection)....415
distinguished-name statement....21, 416
dlv....919, 932
DNS....920
dns statement....417
DNSSEC....919, 921
docsis
profile....168, 189
documentation
comments on....xlii
domain-name statement....21
domain-type statement....71
dot1x statement
WLAN....966
dot1x-supplicant statement
WLAN....967
download
application-identification package....865
download-profile (ftp antivirus utm-profile)....418
download-profile (ftp content-filtering
utm-profile)....418
download-timeout statement....419
drop (gtp)....420
drop statement....424, 645
dropped-packet statement....552
dscp-rewrite....866
dtim-period statement
WLAN....967
duration statement....196
dynamic statement....426
dynamic-attack-group statement....428
dynamic-call-admission-control statement....163
dynamic-vpn statement....427

E

early-ageout statement....429
email-notify....429
enable-all-qmodules statement....430
enable-heuristics statement....866
enable-packet-pool statement....430
encapsulation statement....164
encryption statement....431
encryption-algorithm statement....432
end-system-configuration-timer statement
ES-IS....230
endpoint-registration-timeout statement....432
engine-not-ready....433

Copyright © 2011, Juniper Networks, Inc.

enrollment statement....434
esis statement....230
establish-tunnels statement....435
ethernet statement
WLAN....968
Event-Options Configuration Statement
Hierarchy....127
event-rate statement....435
exceeding-rate-limit statement....552
exception (antivirus mime-whitelist)....436
exception (content-filter block-mime)....436
exclude statement....259
exclude-context-values statement....437
expression statement....438
external statement
WLAN....969
external-interface statement
(IKE Gateway)....438
(Manual Security Association)....439

F

fabric-options statement....164
fail statement....22
fallback-block....439
fallback-block (Sophos)....440
fallback-options (antivirus
juniper-express-engine)....441
fallback-options (antivirus
kaspersky-lab-engine)....442
fallback-options (sophos-engine)....443
fallback-settings (web-filtering juniper-local)....444
fallback-settings (web-filtering
surf-control-integrated)....443
fallback-settings (web-filtering
websense-redirect)....444
false-positives statement....445
family bridge statement....165
family inet statement....166
family inet6 statement....167
family statement....446
feature-profile....447
file statement....810
filename-extension....450
filters statement....451
fin-no-ack statement....452
Firewall Configuration Statement Hierarchy....129
firewall filters
statistics
clearing 1479
displaying....1569, 1586
firewall-authentication statement....23
(Policies)....452
(Security)....453
firewall-authentication-service statement....921
firewall-user statement....24
fixed-multicast-rate statement
WLAN....970
flag statement....810, 898
flood statement
(ICMP)....455
(UDP)....456
flow statement....810
(IDP)....457
(Security Flow)....458
flow-control statement....169
font conventions....xli
force-upgrade statement....459
format statement, first use....459
format statement, second use....460
forwarders 922
forwarding-classes (Cos)....112
Forwarding-Options Configuration Statement
Hierarchy....135
forwarding-options statement....460
forwarding-process....461
fragment statement....461
fragmentation-threshold statement
WLAN....970
framing statement....81
friday statement....260
from statement....462
from-zone statement
(IDP Policy)....462
(Security Policies)....463
ftp statement....24, 465
functional-zone statement....467

G

gatekeeper statement....468
gateway statement
(IKE)....469
(Manual Security Association)....470
general-authentication-service statement....922
Gi interface....482
global-mac-limit statement....232

Copyright © 2011, Juniper Networks, Inc.

global-mac-table-aging-time statement.....233
global-no-mac-learning statement.....233
global-threshold statement.....82
global-weight statement.....83
Gp interface.....482
gprs statement.....480
graceful-restart statement
ES-IS.....231
gratuitous-arp-count statement.....84
gre-in statement.....471
gre-out statement.....472
group statement.....923
group VPN.....473
group-members statement.....476
group-profile statement.....25
group-vpn statement
security.....477
Groups Configuration Statement Hierarchy.....141
gsm-options statement.....170
gtp statement.....480
guard-band statement.....197

H

h323 statement.....483
handshake-timeout statement.....484, 645, 702
hardware
supported platforms.....xl
hash-key statement.....139
header-length statement.....484
heartbeat-interval statement.....85
heartbeat-threshold statement.....86
high-watermark statement.....486
hit-rate-threshold statement.....485
hold-down-interval statement.....87
hold-time statement
ES-IS.....231
host.....486
host (IDP Sensor Configuration) statement.....487
host (Security Logging) statement.....487
host-address-base statement.....488
host-inbound-traffic statement.....488
hostname statement.....489
http statement.....26
http-profile (content-filtering utm-policy).....490
http-profile (web-filtering utm-policy).....490
http-redirect statement
WLAN.....970

I

icmp statement
(Protocol Binding Custom Attack).....490
(Security Screen).....491
(Signature Attack).....492
icmp-code statement.....63
icmp-type statement.....63
identification statement
(ICMP Headers in Signature Attack).....493
(IP Headers in Signature Attack).....493
idle-time statement.....494
idp statement.....495
idp-policy statement.....502
ids-option statement.....504
ignore-mem-overflow statement.....505
ignore-regular-expression statement.....506
ike statement
(IPsec VPN).....509
(Security).....510
group VPN.....508
member.....507
ike-policy statement.....512
ike-user-type statement.....512
imap-profile (antivirus utm-policy).....513
imap-profile (content-filtering utm-policy).....513
IMSI prefix (gtp).....570
inactive-media-timeout statement
(MGCP).....514
(SCCP).....514
(SIP).....515
inactivity-timeout statement.....64, 515
include-destination-address statement.....516
Index is the statement name. Example - action
statement.....91, 517
inet statement.....516
inet6 statement.....517
infranet-controller statement.....871
inline-tap.....518
install-interval statement.....518
intelligent-prescreening.....519
interface (Cos).....113
interface statement.....88, 198, 872, 924
(ARP Proxy Services Gateway).....519
(source NAT).....520
bridge domain.....72
ES-IS.....232
interface-monitor statement.....89
interface-traceoptions statement
DHCP local server.....925

Copyright © 2011, Juniper Networks, Inc.

Interfaces Configuration Statement Hierarchy.....143
interfaces statement.....521
interval (juniper-express-engine).....523
interval (kaspersky-lab-engine).....522
interval (pattern-update).....523
interval statement.....199, 873
(IDP).....521
(IKE).....522
ip statement
(Protocol Binding Custom Attack).....524
(Security Screen).....525
(Signature Attack).....527
ip-action statement.....528
application-level DDoS.....529
ip-block statement.....529
ip-close statement.....530
ip-connection-rate-limit statement.....530
ip-flags statement.....531
ip-monitoring statement.....90
ip-notify statement.....531
ip-sweep statement.....536
ips statement.....532
ipsec statement
group VPN
server.....533
ipsec-group-vpn statement
group VPN.....534
ipsec-policy statement.....534
ipsec-vpn statement
(Dynamic VPNs).....536
(Flow).....535
(Policies).....535
iso statement.....537
isup statement.....424

J

juniper-express-engine.....538
juniper-local.....539

K

kaspersky-lab-engine.....540

L

l2-learning statement.....234
lacp statement.....171
land statement.....541
large statement.....541
latency (radio-router).....171
ldap-options statement.....27
ldap-server statement.....28
lease-time statement.....172
lifetime-kilobytes statement.....542
lifetime-seconds statement
group VPN.....542
IKE.....543
IPsec.....543
limit.....544
limit statement.....545, 645
limit-session statement.....546
link statement.....28
link-speed statement.....173
list (antivirus mime-whitelist).....546
list (content-filter block-mime).....547
local statement.....547
local-address statement
group VPN
member.....548
local-certificate statement.....548
local-identity statement.....549
log statement.....552, 702
(GTP).....550
(IDP Policy).....551
(IDP).....551
(Security Logging).....553
(Security Policies).....552
log-attacks statement.....554
log-errors statement.....554
log-supercede-min statement.....555
login statement.....29
loopback statement.....173
low-watermark statement.....555

M

m3ua-service statement.....424, 645
mac-authentication-type statement
WLAN.....972
management statement.....199, 556
management-vlan statement
WLAN.....972
manual statement.....557
manuals
comments on.....xlii
match statement
(Destination NAT Services Gateway).....558
(IDP Policy).....559, 560
(Security Policies).....560
(Source NAT Services Gateway).....561
max-checked-bytes statement.....873

Copyright © 2011, Juniper Networks, Inc.

max-context-values statement....562
max-flow-mem statement....562
max-logs-operate statement....563
max-packet-mem statement....564
max-packet-memory statement....564
max-session-number statement....565
max-sessions statement....565
max-tcp-session-packet-memory statement....566
max-time-report statement....567
max-timers-poll-ticks statement....567
max-udp-session-packet-memory
statement....568
maximize-alg-sessions....347
maximize-cp-sessions....347
maximize-idp-sessions....347, 568
maximum-burst statement
WLAN....973
maximum-call-duration statement....569
maximum-contention-window statement
WLAN....974
maximum-message-length statement....569
maximum-power statement....200
maximum-stations statement
WLAN....973
max–message-length (gtp)....563
mcc-mnc (gtp)....570
media-source-port-any statement....571
member statement....573
group VPN....572
member-interfaces statement....174
message-flood statement
(H323)....574
(MGCP)....574
mgcp statement....575
mime-pattern....576
mime-whitelist....577
minimum-contention-window statement
WLAN....974
minimum-links statement....175
min–message-length (gtp)....578
mode (Security Logging) statement....580
mode statement
(Forwarding Options)....579
(Policy)....580
WLAN....975
monday statement....261
mpls statement....581
msrpc statement....582
mss statement....583

N

name-server statement
WLAN....976
nat statement
(Services Gateway Configuration)....584
nat-keepalive statement....586
native-vlan-id statement....175
negate statement....586
neighbor-discovery-router-advertisement
statement....30
nested-application services....875
nested-application-identification....587
nested-application-system-cache....587
network-security statement....926
next-hop-tunnel statement....176
no-acknowledgement statement
WLAN....976
no-allow-icmp-without-flow statement....587
no-anti-replay statement....588
no-application-identification statement....876
no-application-system-cache statement
(Services)....876
no-auto-power-save statement
WLAN....977
no-autoupdate (sophos-engine)....588
no-broadcast-ssid statement
WLAN....977
no-enable-all-qmodules statement....588
no-enable-packet-pool statement....588
no-flow-control statement....176
no-log-errors statement....588
no-loopback statement....176
no-nat-traversal statement....589
no-notify-mail-recipient....589
no-notify-mail-sender (fallback-block)....590
no-notify-mail-sender (virus-detection)....590
no-policy-lookup-cache statement....590
no-reset-on-policy statement....590
no-sequence-check statement....591
no-short-guard-interval-supported statement
WLAN....977
no-source-filtering statement....176
no-syn-check statement....591
no-syn-check-in-tunnel statement....592
no-unframed option 190
no-uri-check....592
no-wifi-multimedia statement
WLAN....978

Copyright © 2011, Juniper Networks, Inc.

node statement
(Cluster)....91
(Redundancy-Group)....92
notice icons....xl
notification statement....593
notification-options (antivirus juniper-express-engine)....594
notification-options (antivirus kaspersky-lab-engine)....595
notification-options (antivirus sophos-engine)....596
notification-options (content-filtering)....597
notify-mail-recipient....597
notify-mail-sender (antivirus fallback-block)....598
ntp-sever statement
WLAN....978

O

optimized statement....599
option statement....599
order statement....600
out-of-resources....600
over-limit....601
overflow-pool statement
;(Source NAT Services Gateway....602
overrides statement
DHCP local server....927

P

packet-action statement....234
packet-capture....603
packet-log statement....605
pair-policy statement....606
parentheses, in syntax descriptions....xlii
parser statement....810
pass-through statement....31, 608
password statement....32, 877
password-file....609
pattern statement....609
pattern-update (juniper-express-engine)....610
pattern-update (kaspersky-lab-engine)....610
pattern-update (sophos-engine)....611
payload-protocol statement....645
peer-certificate-type statement....612
perfect-forward-secrecy statement....612
performance statement....613
periodic statement....177
permit statement....615
persistent NAT....614
permit-command....616
persistent-nat statement....616
pic-mode....178
pic-mode (channel) statement....94
pic-mode statement....93
ping-death statement....617
pki statement....618
pki-local-certificate statement....928
PoE configuration statement hierarchy....195
policers, displaying....1540
policies statement....620
policies, displaying....1495
policy statement
(IKE)....622
policy statement: (Security)....624
policy-lookup-cache statement....625
Policy-Options Configuration Statement Hierarchy....203
policy-rematch statement....625
pool statement....33
(Destination NAT Services Gateway)....626
(Source NAT Services Gateway)....626
pool-utilization-alarm statement....627
pop3-profile (antivirus utm-policy)....627
pop3-profile (content-filtering utm-policy)....628
port (web filtering)....629
port statement....628, 878
(LDAP)....34
(RADIUS)....35
port-randomization statement
(source NAT)....629
port-scan statement....630
post-attack statement....631
post-attack-timeout statement....631
pptp statement....632
pre-attack statement....633
pre-filter-shellcode statement....633
pre-shared-key statement....635
predefined-attack-groups statement....634
predefined-attacks statement....634
preempt statement....94
preference statement
ES-IS....235
prefix statement....35
priority statement....95, 201
process-ignore-s2c statement....635
process-override statement....636
process-port statement....636

Copyright © 2011, Juniper Networks, Inc.

processes
restarting....1134
products statement....637
profile (antispam sbl)....637
profile (antivirus juniper-express-engine)....639
profile (antivirus kaspersky-lab-engine)....638
profile (antivirus sophos-engine)....640
profile (content-filtering)....641
profile (gtp)....642
profile (web-filtering juniper-local)....648
profile (web-filtering
surf-control-integrated)....646
profile (web-filtering websense-redirect)....647
profile statement....36, 645
profiles statement....179
promiscuous-mode statement....179
propagate-settings statement....928
proposal statement....649
proposal-set statement
(IKE)....650
(IPsec)....651
proposals statement....652
protect statement....652
protection statement
WLAN....978
protocol statement....65
(IP Headers in Signature Attack)....654
(IPsec)....653
(Manual Security Association)....653
(Signature Attack)....655
protocol-binding statement....658
protocol-command....659
protocol-name statement....659
Protocols Configuration Statement Hierarchy....207
protocols statement
(Interface Host-Inbound Traffic)....660
(Zone Host-Inbound Traffic)....662
proxy-arp statement
(Services Gateway Configuration)....663
proxy-identity statement....663

Q

quality (radio-router)....180
quality-of-service statement
WLAN....979

R

radio statement
WLAN....981
radio-off statement
WLAN....983
radio-options statement
WLAN....984
radio-router....180
radius-options statement....37
radius-server statement....38
raise-threshold statement....664
range statement....39
rate statement....545, 645
rate-limit (gtp)....664
re-assembler statement....666
re-enroll-trigger-time-percentage statement....666
real statement....665
recommended statement....667
recommended-action statement....667
reconfigure statement
DHCP local server....929
redirect-traffic statement....879, 880
redundancy-group statement....96, 181
redundant-ether-options statement....181
redundant-parent statement
(Fast Ethernet Options)....182
(Gigabit Ethernet Options)....182
regexp statement....668
reject statement....668
reject-timeout statement....669
remote statement....669
remote-exceptions statement....670
remote-protected-resources statement....670
remove-r6 (gtp)....671
request chassis cluster failover node
command....1095
request chassis cluster failover reset
command....1096
request modem wireless activate iota
command....1097
request modem wireless activate manual
command....1098
request modem wireless activate otasp
command....1100
request modem wireless gsm sim-unblock
command....1101
request modem wireless gsm sim-unlock
command....1102
request security datapath-debug capture start
command....1103
request security datapath-debug capture stop
command....1104

Copyright © 2011, Juniper Networks, Inc.

request security idp security-package download command....1105
request security idp security-package install command....1107
request security idp ssl-inspection key add command....1109
request security idp ssl-inspection key delete command....1111
request security pki ca-certificate verify command....1113
request security pki local-certificate generate-self-signed command....1114
request security pki local-certificate verify command....1116
request security utm anti-virus juniper-express-engine....1117
request security utm anti-virus kaspersky-lab-engine....1118
request security utm anti-virus sophos-engine....1119
Request services application identification download command....1092
Request services application identification download status command....1093
request services application-identification uninstall command....1094
request system license update command....1120
request system partition compact-flash command....1121
request system services dhcp command....1122
request system snapshot partition....1123
request system software add 1124
request system software in-service-upgrade command....1125
request system software reboot....1127
request system software rollback....1128
request wan-acceleration login command....1129
request wlan access-point firmware upgrade command....1130
request wlan access-point restart command....1132
reset statement....671
reset-on-policy statement....672
resource (radio-router)....183
respond-bad-spi statement....672
restart command....1134
restart-duration statement
ES-IS....231
restarting
software processes....1134
retain-hold-resource statement....673
reth-count statement....98
retransmission-attempt statement....183
retransmission-interval statement....184
retry statement
(LDAP)....39
(RADIUS)....40
retry-count statement....97
retry-interval statement....98
reverse ssh....930
reverse ssh port....930
reverse telnet....931
reverse telnet port....931
revert-interval statement
(LDAP)....40
(RADIUS)....41
revocation-check statement....673
roaming-mode statement....184
route-active-on statement....205
route-change-timeout statement....674
routing-instance statement
(Destination NAT Services Gateway)....674
(LDAP)....41
(RADIUS)....42
(Source NAT Services Gateway)....675
Routing-Instances Configuration Statement Hierarchy....239
routing-interface statement....72
Routing-Options Configuration Statement Hierarchy....249
rpc statement....675
rpc-program-number statement....66
rsh statement....676
rst-invalidate-session statement....677
rst-sequence-check statement....677
rts-threshold statement
WLAN....985
rtsp statement....678
rule statement
(destination NAT)....681
(Exempt Rulebase)....682
(IPS Rulebase)....683
(Source NAT)....684
DDoS Rulebase....680
rule-set statement
(Destination NAT Services Gateway)....688
(Source NAT Services Gateway)....689
rulebase-ddos statement....686
rulebase-exempt statement....691
rulebase-ips statement....692

Copyright © 2011, Juniper Networks, Inc.

S

saturday statement....262
sbl....693
sbl-default-server....694
scan-mode....694
scan-options (anti-virus
kaspersky-lab-engine)....695
scan-options (antivirus
juniper-express-engine)....695
sccp statement....424, 545, 696
scheduler statement....263
scheduler-name statement....697
schedulers statement....264
scope statement
(Chain Attack)....697
(Custom Attack)....698
screen statement
(Security)....699
(Zones)....701
sctp statement....350, 484, 552, 645, 702, 810
search statement....42
search-filter statement....43
secondary-server statement....899
secret statement....43
securid-server statement....44
Security Configuration Statement Hierarchy....273
security statement
WLAN....986
security-package statement....703
security-zone statement....704
select-profile statement....185
sensor-configuration statement....705
separator statement....45
seq-number-validated (gtp)....706
sequence-number statement
(ICMP Headers in Signature Attack)....710
(TCP Headers in Signature Attack)....710
server....707
server statement
group VPN....711
server-address statement....185
server-certificate-subject statement....881
server-connectivity....707
service statement
(Anomaly Attack)....713
(DDoS)....713
(Dynamic Attack Group)....714
(Security IPsec)....714
Services Configuration Statement Hierarchy....857
session-close statement....708
session-init statement....709
session-options statement....45
sessions statement....708
sessions-per-client....709
severity statement
(Custom Attack)....716
(Dynamic Attack Group)....717
(IPS Rulebase)....718
shellcode statement....719
show bgp neighbor command....1138
show chassis cluster control-plane statistics
command....1143
show chassis cluster data-plane interfaces
command....1145
show chassis cluster data-plane statistics
command....1146
show chassis cluster ethernet-switching interfaces
command....1160
show chassis cluster ethernet-switching status
command....1161
show chassis cluster interfaces command....1148
show chassis cluster ip-monitoring status
redundancy-group command....1150
show chassis cluster statistics command....1153
show chassis cluster status command....1157
show chassis fpc command....1163
show chassis hardware command....1166
show configuration smtp 1142
show dhcpv6 server binding....1171
show dhcpv6 server statistics command....1175
show esis adjacency command....1177
show esis interface command....1179
show esis statistics command....1181
show ethernet-switching mac-learning-log
command....1183
show ethernet-switching table command....1185
show gtp tunnels....1189
show igmp-snooping route command....1190
show igmp-snooping vlans command....1192
show interfaces (Aggregated Ethernet)
command....1200
show interfaces command....1194
show interfaces flow-statistics command....1212
show interfaces swfabx command....1216
show lacp interfaces command....1217
show lacp statistics interfaces command....1221
show modem wireless interface command....1222

Copyright © 2011, Juniper Networks, Inc.

show modem wireless interface firmware command....1224
show modem wireless interface network command....1226
show modem wireless interface rssi command....1228
show network-access address-assignment pool command....1229
show network-access requests pending command....1230
show network-access requests statistics command....1232
show network-access securid-node-secret-file command....1233
show poe controller command....1234
show poe interface command....1235
show poe telemetries interface....1237
show schedulers command....1239
show security alg h323 counters command....1241
show security alg ike-esp-nat summary command....1243
show security alg mgcp calls command....1244
show security alg mgcp counters command....1246
show security alg mgcp endpoints command....1249
show security alg msrpc command....1251
show security alg sccp calls command....1252
show security alg sccp counters command....1254
show security alg sip calls command....1256
show security alg sip counters command....1258
show security alg sip rate command....1262
show security alg sip transactions command....1264
show security alg status command....1265
show security application-firewall rule-set command....1267
show security application-tracking counters command....1269
show security datapath-debug capture....1270
show security datapath-debug counter....1271
show security dynamic-policies command....1272
show security dynamic-vpn client version....1277
show security dynamic-vpn users....1278
show security dynamic-vpn users terse....1279
show security firewall-authentication history address command....1282
show security firewall-authentication history command....1280
show security firewall-authentication history identifier command....1285
show security firewall-authentication users address command....1290
show security firewall-authentication users command....1288
show security firewall-authentication users identifier command....1292
show security flow cp-session command....1294
show security flow cp-session destination-port command....1296
show security flow cp-session destination-prefix command....1298
show security flow cp-session family command....1300
show security flow cp-session protocol command....1302
show security flow cp-session source-port command....1304
show security flow cp-session source-prefix command....1306
show security flow gate brief node command....1312
show security flow gate command....1308
show security flow gate destination-port command....1318
show security flow gate destination-prefix command....1321
show security flow gate family command....1324
show security flow gate protocol command....1326
show security flow gate source-port command....1329
show security flow gate source-prefix command....1332
show security flow gate summary node command....1335
show security flow ip-action....1340
show security flow ip-action family command....1341
show security flow session application command....1346
show security flow session brief node command....1350
show security flow session command....1342
show security flow session destination-port command....1354
show security flow session destination-prefix command....1358
show security flow session extensive node command....1362
show security flow session interface command....1374

Copyright © 2011, Juniper Networks, Inc.

show security flow session protocol command....1382
show security flow session resource-manager command....1387
show security flow session session-identifier command....1391
show security flow session source-port command....1394
show security flow session source-prefix command....1398
show security flow session summary family command....1402
show security flow session summary node command....1404
show security flow session tunnel command....1409
show security gprs sctp counters command....1415
show security group-vpn member ike security-associations command....1416
show security group-vpn member ipsec security-associations command....1420
show security group-vpn member kek security-associations command....1423
show security group-vpn server ike security-associations command....1426
show security group-vpn server ipsec security-associations command....1430
show security group-vpn server kek security-associations command....1434
show security group-vpn server registered-members command....1438
show security idp active-policy command....1440
show security idp application-ddos command....1441
show security idp application-identification application-system-cache command....1443
show security idp attack table command....1444
show security idp counters application-ddos command....1445
show security idp counters application-identification command....1448
show security idp counters dfa command....1450
show security idp counters flow command....1451
show security idp counters ips command....1454
show security idp counters log command....1456
show security idp counters packet command....1459
show security idp counters packet-log command....1462
show security idp counters policy-manager command....1464
show security idp counters tcp-reassembler command....1465
show security idp memory command....1468
show security idp policies....1469
show security idp policy-templates....1470
show security idp predefined-attacks....1471
show security idp security-package-version command....1473
show security idp ssl-inspection key command....1474
show security idp ssl-inspection session-id-cache command....1475
show security idp status command....1476
show security idp status detail....1477
show security ike pre-shared-key command....1478
show security ike security-associations command....1479
show security ipsec next-hop-tunnels command....1485
show security ipsec security-associations command....1486
show security ipsec statistics command....1492
show security match-policies command....1495
show security monitoring fpc fpc-number command....1499
show security nat destination pool command....1503
show security nat destination rule command....1505
show security nat destination summary command....1508
show security nat incoming-table command....1510
show security nat interface-nat-ports command....1512
show security nat source persistent-nat-table command....1514
show security nat source pool command....1517
show security nat source rule command....1519
show security nat source summary command....1522
show security nat static-nat summary command....1526
show security pki ca-certificate command....1528
show security pki certificate-request command....1532
show security pki crl command....1534
show security pki local-certificate command....1536
show security policies command....1540

Copyright © 2011, Juniper Networks, Inc.

show security resource-manager group active command....1544
show security resource-manager resource active command....1546
show security resource-manager settings command....1548
show security screen ids-option command....1550
show security screen statistics command....1553
show security softwires 1558
show security utm anti-spam statistics....1559
show security utm anti-spam status....1560
show security utm anti-virus statistics....1561
show security utm anti-virus status....1562
show security utm content-filtering statistics....1564
show security utm session....1565
show security utm status....1566
show security utm web-filtering statistics....1567
show security utm web-filtering status....1568
show security zones command....1569
show security zones type command....1571
show services accounting aggregation command....1574
show services accounting aggregation template command....1575
show services accounting command....1573
show services accounting flow-detail command....1576
show services application-identification application-system-cache command....1577
show services application-identification counter command....1579
show services application-identification version....1581
show services unified-access-control authentication-table command....1582
show services unified-access-control policies command....1583
show services unified-access-control status command....1585
show system services dhcp client command....1586
show system services dhcp relay-statistics command....1589
show system snapshot media....1591
show system storage partitions....1592
show wan-acceleration status command....1593
show wlan access-points command....1594
signature statement....720
(application identification)....882
sip statement....724
sip-password statement....186
sip-user-id statement....187
SMTP Configuration Statement Hierarchy....897
smtp-profile (antispam utm-policy)....725
smtp-profile (antivirus utm-policy)....725
smtp-profile (content-filtering utm-policy)....725
SNMP Configuration Statement Hierarchy....891
sockets....726
sophos-engine....727
source statement
(IP Headers in Signature Attack)....728
(Source NAT Services Gateway)....729
source-address statement
(Destination NAT Services Gateway)....730
(IDP Policy)....731
(LDAP)....46
(RADIUS)....46
(Security Policies)....732
(Source NAT Services Gateway)....732
source-address-filter statement....187
source-except statement....733
source-filtering statement....188
source-interface statement....733
source-ip-based statement....734
source-nat statement: (Source NAT Services Gateway)....735
source-port statement....66, 736
source-threshold statement....737
space-time-block-coding statement
WLAN....987
spam-action....737
speed
profile....188
spi statement....738
sql statement....739
ssh-known-hosts statement....740
ssid statement
WLAN....987
ssl-inspection statement....741
ssp statement....545
sst statement....545
start-date statement....264
start-log statement....741
start-time statement....265, 742
static statement....742
WLAN....987
static-mac statement....73

Copyright © 2011, Juniper Networks, Inc.

static-wep statement
WLAN....988
station-mac-filter statement
WLAN....989
station-queues statement
WLAN....990
statistics statement....743
stop-date statement....266
stop-time statement....267
strict-syn-check statement....744
success statement....47
sunday statement....268
sunrpc statement....744
support, technical *See* technical support
suppression statement....745
surf-control-integrated....746
sxl-retry....747
sxl-timeout....747
syn-ack-ack-proxy statement....748
syn-fin statement....748
syn-flood statement....749
syn-flood-protection-mode statement....749
syn-frag statement....750
syntax conventions....xli
syslog-options statement
WLAN....991
System Configuration Statement Hierarchy....901
system-generated-certificate statement....932
system-services statement
(Interface Host-Inbound Traffic)....751
(Zone Host-Inbound Traffic)....753

T

t1-interval statement....754
t3-options statement
no-unframed option....190
unframed option....190
t4-interval statement....755
talk statement....756
target statement....757
tcp statement
(Protocol Binding Custom Attack)....758
(Security Screen)....759
(Signature Attack)....760
tcp-flags statement....762
tcp-initial-timeout statement....763
tcp-mss statement....764
tcp-no-flag statement....765
tcp-rst statement....765
tcp-session statement....766
tcp-sweep statement....767
technical support
contacting JTAC....xlii
telemetries statement....202
telnet statement....47
term statement....67
terminal statement....767
test statement....768
test-only-mode statement....884
tftp statement....769
then statement
(Destination NAT Services Gateway)....770
(IDP Policy)....771, 772
(Security Policies)....773
(Source NAT Services gateway)....774
threshold (radio-router)....189
threshold statement....775
thursday statement....269
time-binding statement....775
time-binding-count statement....776
time-binding-period statement....777
timeout (antivirus fallback-options)....779
timeout (antivirus scan-options)....780
timeout (gtp)....778
timeout (web-filtering fallback-settings)....781
timeout (web-filtering surf-control-integrated cache)....780
timeout (web-filtering websense-redirect profile)....781
timeout statement....885
(IDP Policy)....778
(LDAP Server)....48
(RADIUS Server)....48
(Security Screen)....779
timeout-action statement....886
to statement....782
to-zone statement....782
too-many-requests (antivirus fallback-options)....783
too-many-requests (web-filtering fallback-settings)....783
tos statement....784
total-length statement....785
traceoption statement....702
traceoptions statement....49, 99, 810, 888, 900
(Application Firewall)....786
(application identification)....887
(firewall-authentication)....787

(Flow)....789
(General Authentication Service)....937
(group VPN)....792
(GTP)....791
(H.323 ALG)....788
(IDP)....794
(IKE)....796
(IPsec)....798
(MGCP ALG)....799
(NAT Services Gateway)....800
(PKI)....803
(Policies)....805
(SCCP ALG)....807
(Screen)....808
(Security)....811
(SIP ALG)....813
(WAN Acceleration)....939
DHCP local server....933
ES-IS....236
tracing flags
ES-IS....236
traffic-options....814
transaction-timeout statement....814
transmit-opportunity-limit statement
WLAN....991
transmit-power statement
WLAN....992
transmit-rate-sets statement
WLAN....992
trickling....815
trigger statement....122
trusted-ca statement....816
trusted-keys....940
ttl statement....817
tuesday statement....270
tunable-name statement....817
tunable-value statement....818
tunnel statement....818
tunnel-queuing statement....100
type (antivirus fallback-block)....820
type (antivirus feature-profile)....820
type (antivirus notification-options
virus-detection)....821
type (content-filtering notification-options)....821
type statement
(Dynamic Attack Group)....819
(ICMP Headers in Signature Attack)....819

U

udp statement
(Protocol Binding Custom Attack)....822
(Security Screen)....823
(Signature Attack)....824
udp-sweep statement....825
unframed option....190
unified-access-control statement....889
unknown-message statement
(H.323.ALG)....826
(MGCP ALG)....827
(SCCP ALG)....828
(SIP ALG)....829
untagged-vlan statement
WLAN....993
update-server statement....190
upload-profile (ftp antivirus utm-profile)....830
upload-profile (ftp content-filtering
utm-profile)....830
urgent-pointer statement....831
uri-check....831
url (juniper-express-engine)....832
url (kaspersky-lab-engine)....832
url (sophos-engine)....833
url statement....832
url-blacklist....833
url-pattern....834
url-whitelist (antivirus)....834
url-whitelist (web-filtering)....835
user statement....835
user-at-hostname statement....836
utm statement....837
utm-policy....842
uuid statement....68

V

value-hit-rate-threshold statement....843
vdsl
profile....192
vendor-id statement....192
video-queue statement
WLAN....993
virtual-access-point statement
WLAN....994
virtual-channel-group statement....124
virtual-channel-groups statement....125
virtual-channels statement....123
virus-detection....844
virus-detection (Sophos)....844

Copyright © 2011, Juniper Networks, Inc.

vlan statement
WLAN....995
vlan-id statement....73
vlan-id-list statement....74
vlan-tagging statement....193
voice-queue statement
WLAN....996
vpn statement....140, 845
vpn-monitor statement....846
vpn-monitor-options statement....847

W

wan-acceleration statement....941
web-authentication statement....51, 193, 848
web-redirect statement....849
wednesday statement....271
weight statement....101
wildcard statement....851
window-scale statement....851
window-size statement....852
winnuke statement....852
WLAN Configuration Statement Hierarchy....943
wpa-enterprise statement
WLAN....997
wpa-personal statement
WLAN....998

X

xauth statement....853

Z

zones statement 854

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.