JUNOS® Software

CLI Reference

Release 10.0

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

Revision 01
Published: 2009-10-07

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, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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® Software CLI Reference
Release 10.0
Copyright © 2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
October 2009—Revision 01

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 Software 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.

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)).

Table of Contents

About This Guide **xxxvii**

J Series and SRX Series Documentation and Release Notes xxxvii
Objectives xxxviii
Audience xxxviii
Supported Routing Platforms xxxviii
How to Use This Manual xxxviii
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
admin-search 6
assemble 7
authentication-order 7
banner 8
banner (FTP, HTTP, Telnet) 8
banner (Web Authentication) 9
base-distinguished-name 9
client-group 10
client-idle-timeout 10
client-name-filter 11
client-session-timeout 11
configuration-file 12
count 12
default-profile 13
distinguished-name 13
domain-name 14
fail 14
firewall-authentication 15
firewall-user 16
ftp 16
http 17
ldap-options 18

ldap-server 19
login 19
pass-through 20
password 21
port 22
port (LDAP) 22
port (RADIUS) 22
radius-options 23
radius-server 24
retry 25
retry (LDAP) 25
retry (RADIUS) 25
revert-interval 26
revert-interval (LDAP) 26
revert-interval (RADIUS) 26
routing-instance 27
routing-instance (LDAP) 27
routing-instance (RADIUS) 27
search 28
search-filter 28
secret 29
securid-server 29
separator 30
session-options 30
source-address 31
source-address (LDAP) 31
source-address (RADIUS) 31
success 32
telnet 32
timeout 33
timeout (LDAP Server) 33
timeout (RADIUS Server) 33
traceoptions 34
web-authentication 35

Chapter 2 Accounting-Options Hierarchy 37

Accounting-Options Configuration Statement Hierarchy 37

Chapter 3 Applications Hierarchy and Statements 39

Applications Configuration Statement Hierarchy 39
alg 41
application-protocol 42
destination-port 43
icmp-code 46
icmp-type 47
inactivity-timeout 47
protocol 48
rpc-program-number 49

source-port 49
term 50
uuid 51

Chapter 4 Bridge-Domains Hierarchy and Statements 53

Bridge-Domains Configuration Statement Hierarchy 53
bridge-domains 54
bridge-options 55
domain-type 55
interface 56
routing-interface 56
static-mac 57
vlan-id 57
vlan-id-list 58

Chapter 5 Chassis Hierarchy and Statements 59

Chassis Configuration Statement Hierarchy 59
cluster 63
control-link-recovery 64
control-ports 65
gratuitous-arp-count 66
heartbeat-interval 66
heartbeat-threshold 67
hold-down-interval 67
interface-monitor 68
ip-monitoring 69
node 70
    node (Cluster) 70
    node (Redundancy-Group) 70
pic-mode 71
preempt 71
priority 72
redundancy-group 73
reth-count 74
threshold 74
traceoptions 75
tunnel-queuing 76
weight 77

Chapter 6 Class-of-Service Hierarchy and Statements 79

Class-of-Service Configuration Statement Hierarchy 79
adaptive-shaper 83
adaptive-shapers 84
code-points (Forwarding Class) 84
default 85
frame-relay-de (Assigning to an Interface) 86

frame-relay-de (Defining Loss Priority) 87
frame-relay-de (Defining Rewrite Rule) 88
loss-priority (Frame Relay DE Bit Loss-Priority Map) 89
loss-priority (Rewrite Rules) 90
loss-priority-maps (Assigning to an Interface) 91
loss-priority-maps (Defining) 91
rewrite-rules (Definition) 92
rewrite-rules (Interfaces) 93
scheduler-map (Virtual Channels) 94
shaping-rate (Adaptive Shaping) 94
shaping-rate (Applying to an Interface) 95
shaping-rate (Virtual Channels) 96
trigger 96
virtual-channels 97
virtual-channel-group 98
virtual-channel-groups 99

Chapter 7 Event-Options Hierarchy 101

Event-Options Configuration Statement Hierarchy 101

Chapter 8 Firewall Hierarchy and Statements 103

Firewall Configuration Statement Hierarchy 103
policer 106
simple-filter 107

Chapter 9 Forwarding-Options Hierarchy and Statements 109

Forwarding-Options Configuration Statement Hierarchy 109
vpn 113

Chapter 10 Groups Hierarchy 115

Groups Configuration Statement Hierarchy 115

Chapter 11 Interfaces Hierarchy and Statements 117

Interfaces Configuration Statement Hierarchy 117
access-point-name 129
activation-priority 130
annex 130
authentication-method 131
bearer-bandwidth-limit 131
bundle 132
cbr rate 132
cellular-options 133

client-identifier 134
compression-device 134
dhcp 135
dynamic-call-admission-control 136
encapsulation 137
fabric-options 138
family bridge 139
flow-control 140
fpc 140
gsm-options 141
interface (PIC Bundle) 141
lease-time 142
line-rate 142
link-speed 143
loopback 143
member-interfaces 144
native-vlan-id 144
next-hop-tunnel 145
no-flow-control 145
no-loopback 145
no-source-filtering 145
pic-mode 146
profiles 146
redundancy-group 147
redundant-ether-options 147
redundant-parent 148
    redundant-parent (Fast Ethernet Options) 148
    redundant-parent (Gigabit Ethernet Options) 148
retransmission-attempt 149
retransmission-interval 149
roaming-mode 150
select-profile 150
server-address 151
simple-filter 151
sip-password 152
sip-user-id 152
source-address-filter 153
source-filtering 154
update-server 154
vbr rate 155
vendor-id 155
vlan-tagging 156
web-authentication 156

Chapter 12 Power Over Ethernet Hierarchy and Statements 157

PoE Configuration Statement Hierarchy 157
disable 158
duration 158
guard-band 159

interface 160
interval 160
management 161
maximum-power 161
priority 162
telemetries 163

Chapter 13 Policy-Options Hierarchy and Statements 165

Policy-Options Configuration Statement Hierarchy 165
condition 167
route-active-on 167

Chapter 14 Protocols Hierarchy and Statements 169

Protocols Configuration Statement Hierarchy 169
disable 192
end-system-configuration-timer 192
esis 193
graceful-restart 193
hold-time 194
interface 194
global-mac-limit 195
global-mac-table-aging-time 195
global-no-mac-learning 196
l2-learning 196
packet-action 197
preference 197
traceoptions 198

Chapter 15 Routing-Instances Hierarchy 201

Routing-Instances Configuration Statement Hierarchy 201

Chapter 16 Routing-Options Hierarchy 213

Routing-Options Configuration Statement Hierarchy 213

Chapter 17 Schedulers Hierarchy and Statements 221

Schedulers Configuration Statement Hierarchy 221
all-day 222
daily 223
exclude 224
friday 225
monday 226
saturday 227

scheduler 228
schedulers 229
start-date 229
start-time 230
stop-date 231
stop-time 232
sunday 233
thursday 234
tuesday 235
wednesday 236

Chapter 18 Security Hierarchy and Statements 237

Security Configuration Statement Hierarchy 237
access profile 267
    access-profile (Dynamic VPNs) 267
    access-profile (IPsec VPNs) 267
ack-number 268
action 269
action (AppDDoS) 270
action (web filtering) 271
active-policy 271
action-profile 272
address 274
    address (ARP Proxy) 274
    address (Destination NAT) 275
    address (IKE Gateway) 275
    address (Zone Address Book) 276
    address (Zone Address Set) 276
address-book 277
address-blacklist 277
address-persistent 278
address-set 278
address-whitelist 279
admin-email 279
administrator 280
aging 280
alarm-threshold 281
alarm-without-drop 281
alert 282
alg 283
algorithm 287
all-tcp 287
allow-dns-reply 288
allow-icmp-without-flow 288
always-send 289
anomaly 289
antispam 290
    antispam (feature-profile) 290
    antispam (utm-policy) 291

antivirus 292
antivirus (feature-profile) 293
antivirus (utm-policy) 295
apn (gtp) 296
application 297
application (AppDDoS) 297
application (Protocol Binding Custom Attack) 297
application (Security Policies) 298
application-identification 298
application-screen 299
application-screen (H323) 299
application-screen (MGCP) 300
application-screen (SCCP) 300
application-screen (SIP) 301
application-services 302
application-services (priority) 302
application-services (Unified Access Control) 303
application-services (WXC Integrated Services Module) 303
application-system-cache 304
application-system-cache-timeout 304
attack-threshold 305
attacks 306
attacks (Exempt Rulebase) 306
attacks (IPS Rulebase) 307
attack-type 308
attack-type (Anomaly) 308
attack-type (Chain) 309
attack-type (Signature) 310
authentication 313
authentication-algorithm 314
authentication-method 315
auto-re-enrollment 316
automatic 316
bind-interface 317
block-command 317
block-content-type 318
block-mime 318
bridge 319
c-timeout 320
ca-identity 320
ca-profile 321
ca-profile-name 322
cache 322
cache-size 323
call-flood 323
category 324
category (Security Logging) 324
category (web filtering) 325
certificate 325
certificate-id 326
chain 327

challenge-password 328
clear-threshold 328
clients 329
code 330
connection-rate-threshold 330
connection-flood 331
connections-limit 331
container 332
content-filtering 333
    content-filtering (feature-profile) 333
    content-filtering (utm-policy) 334
content-size 334
content-size-limit 335
context 335
context (AppDDoS) 336
corrupt-file 336
count 337
    count (Custom Attack) 337
    count (Security Policies) 337
crl 338
custom-attack 339
custom-attack-group 343
custom-attacks 343
custom-block-message 344
custom-message 345
    custom-message (antivirus notification-options fallback-block/non-block) 345
    custom-message (antivirus notification-options virus-detection) 345
    custom-message (content-filter notification-options) 346
custom-message-subject 347
    custom-message-subject (antivirus notification-options fallback-block/non-block) 347
    custom-message-subject (antivirus notification-options virus-detection) 347
    custom-message-subject (antivirus pattern-update email-notify) 348
custom-objects 349
custom-tag-string 349
custom-url-category 350
data-length 350
datapath-debug 351
dead-peer-detection 352
decompress-layer 352
decompress-layer-limit 353
default 354
    default (antivirus fallback-options) 354
    default (web-filtering fallback-settings) 355
default-policy 355
deny 356
    deny (Policy) 356
    deny (SIP) 357

description 358
description (IDP Policy) 358
description (Security Policies) 358
destination 359
destination (Destination NAT) 359
destination (IP Headers in Signature Attack) 360
destination-address 361
destination-address (Destination NAT) 361
destination-address (IDP Policy) 362
destination-address (Security Policies) 362
destination-address (Source NAT) 363
destination-address (Static NAT) 363
destination-address (Traffic Policy Services Gateway) 364
destination-except 364
destination-ip 365
destination-ip-based 365
destination-nat 366
destination-port 367
destination-port (Destination NAT) 367
destination-port (Signature Attack) 367
destination-threshold 368
detect-shellcode 368
detector 369
df-bit 369
dh-group 370
direction 371
direction (Custom Attack) 371
direction (Dynamic Attack Group) 372
disable-call-id-hiding 372
distinguished-name 373
dns 374
download-profile 375
download-profile (ftp antivirus utm-profile) 375
download-profile (ftp content-filtering utm-profile) 375
drop (gtp) 376
dynamic 379
dynamic-vpn 380
dynamic-attack-group 381
early-ageout 382
email-notify 382
enable-all-qmodules 383
enable-packet-pool 383
encryption 384
encryption-algorithm 385
endpoint-registration-timeout 385
engine-not-ready 386
enrollment 387
establish-tunnels 388
event-rate 388

exception 389
exception (antivirus mime-whitelist) 389
exception (content-filter block-mime) 389
exclude-context-values 390
expression 391
external-interface 392
external-interface (IKE Gateway) 392
external-interface (Manual Security Association) 392
fallback-block 393
fallback-options 394
fallback-options (antivirus juniper-express-engine) 394
fallback-options (antivirus kaspersky-lab-engine) 395
fallback-settings 396
fallback-settings (web-filtering surf-control-integrated) 396
fallback-settings (web-filtering websense-redirect) 397
fallback-settings (web-filtering juniper-local) 397
false-positives 398
family 399
feature-profile 400
filename-extension 403
filters 404
fin-no-ack 405
firewall-authentication 406
firewall-authentication (Policies) 406
firewall-authentication (Security) 407
flood 408
flood (ICMP) 408
flood (UDP) 409
flow 410
flow (IDP) 410
flow (Security Flow) 411
force-upgrade 412
format (first use in Security Logging) 412
format (second use in Security Logging) 413
forwarding-options 413
forwarding-process 414
fragment 414
from 415
from-zone 416
from-zone (IDP Policy) 416
from-zone (Security Policies) 417
ftp 418
ftp (utm) 419
ftp (antivirus utm-policy) 419
ftp (content-filtering utm-policy) 419
functional-zone 420
gatekeeper 421
gateway 422
gateway (IKE) 423
gateway (IPsec) 424
gateway (Manual Security Association) 424

global 425
gre-in 425
gre-out 426
group-members 427
gtp 428
h323 431
header-length 432
hit-rate-threshold 433
high-watermark 434
host 434
host (Security Logging) 435
host-address-base 435
host-inbound-traffic 436
hostname 436
http-profile 437
    http-profile (antivirus utm-policy) 437
    http-profile (content-filtering utm-policy) 437
    http-profile (web-filtering utm-policy) 438
icmp 439
    icmp (Protocol Binding Custom Attack) 439
    icmp (Security Screen) 440
    icmp (Signature Attack) 441
identification 442
    identification (ICMP Headers in Signature Attack) 442
    identification (IP Headers in Signature Attack) 443
idle-time 443
idp 444
idp-policy 451
ids-option 453
ignore-mem-overflow 454
ignore-regular-expression 455
ike 456
    ike (IPsec VPN) 456
    ike (Security) 457
ike-policy 458
ike-user-type 459
imap-profile 460
    imap-profile (antivirus utm-policy) 460
    imap-profile (content-filtering utm-policy) 460
inactive-media-timeout 461
    inactive-media-timeout (MGCP) 461
    inactive-media-timeout (SCCP) 461
    inactive-media-timeout (SIP) 462
include-destination-address 462
inet 463
inet6 463
install-interval 464
intelligent-prescreening 464
interface 465
    interface (ARP Proxy) 465
    interface (Source NAT) 465

interfaces 466
interval 467
interval (IDP) 467
interval (IKE) 467
interval (anti-virus) 468
interval (kaspersky-lab-engine) 468
interval (juniper-express-engine) 468
ip 469
ip (Protocol Binding Custom Attack) 469
ip (Security Screen) 470
ip (Signature Attack) 472
ip-action 473
ip-action (AppDDoS) 474
ip-block 474
ip-close 475
ip-flags 475
ip-notify 476
ips 476
ipsec-policy 477
ipsec-vpn 478
ipsec-vpn (Flow) 478
ipsec-vpn (Policies) 478
ipsec-vpn (Dynamic VPNs) 479
ip-sweep 479
iso 480
juniper-express-engine 481
juniper-local 482
kaspersky-lab-engine 483
land 484
large 484
lifetime-kilobytes 485
limit 485
limit-session 486
list 487
list (antivirus mime-whitelist) 487
list (content-filter block-mime) 487
local 488
local-certificate 488
local-identity 489
log 490
log (GTP) 491
log (IDP) 492
log (IDP Policy) 492
log (Security Policies) 493
log (Security Logging) 494
log-attacks 495
log-errors 495
log-supercede-min 496
low-watermark 496
management 497
manual 498

match 499
match (Destination NAT) 499
match (IDP Policy) 500
match (rulebase-ddos) 501
match (Security Policies) 501
match (Source NAT) 502
match (Static NAT) 502
max-context-values 503
max-flow-mem 503
max-logs-operate 504
max–message–length 504
max-packet-mem 505
max-packet-memory 505
max-sessions 506
max-tcp-session-packet-memory 506
max-time-report 507
max-timers-poll-ticks 507
max-udp-session-packet-memory 508
maximize-idp-sessions 508
maximum-call-duration 509
mcc–mnc (gtp) 510
media-source-port-any 511
member 511
message-flood 512
message-flood (H323) 512
message-flood (MGCP) 513
mgcp 514
mime-pattern 515
mime-whitelist 515
min–message–length 516
mode 517
mode (Forwarding-Options) 517
mode (Policy) 517
mode (Security Logging) 518
mpls 518
msrpc 519
mss 520
nat 521
nat-keepalive 523
negate 523
no-allow-icmp-without-flow 524
no-anti-replay 524
no-enable-all-qmodules 524
no-enable-packet-pool 524
no-log-errors 524
no-nat-traversal 525
no-policy-lookup-cache 525
no-reset-on-policy 525
no-sequence-check 525
no-syn-check 526
no-syn-check-in-tunnel 526

notification 527
notification-options 528
notification-options (antivirus juniper-express-engine) 528
notification-options (antivirus kaspersky-lab-engine) 529
notification-options (content-filtering) 529
notify-mail-sender 530
notify-mail-sender (antivirus fallback-block) 530
notify-mail-sender (antivirus notification-options virus-detection) 530
optimized 531
option 531
order 532
out-of-resources 532
over-limit 533
overflow-pool 533
packet-filter 534
pair-policy 535
pass-through 536
password-file 537
pattern 537
pattern-update 538
pattern-update (kaspersky-lab-engine) 538
pattern-update (juniper-express-engine) 539
peer-certificate-type 539
perfect-forward-secrecy 540
performance 541
permit 542
permit-command 543
persistent-nat 544
ping-death 545
pki 546
policies 548
policy 550
policy (IKE) 550
policy (IPsec) 551
policy (Security) 552
policy-lookup-cache 553
policy-rematch 553
pool 554
pool (Destination NAT) 554
pool (Source NAT) 555
pool-utilization-alarm 555
pop3–profile 556
pop3-profile (antivirus utm-policy) 556
pop3-profile (content-filtering utm-policy) 556
port 557
port (web filtering) 557
port-randomization 558
port-scan 559
pptp 560
pre-filter-shellcode 560
predefined-attack-groups 561

predefined-attacks 561
pre-shared-key 562
process-ignore-s2c 562
process-override 563
process-port 563
products 564
profile 565
profile (antispam sbl) 565
profile (antivirus kaspersky-lab-engine) 566
profile (antivirus juniper-express-engine) 567
profile (content-filtering) 568
profile (gtp) 569
profile (web-filtering surf-control-integrated) 571
profile (web-filtering websense-redirect) 572
profile (web-filtering juniper-local) 573
proposal 574
proposal-set 575
proposal-set (IKE) 575
proposal-set (IPsec) 576
protect 577
protocol 578
protocol (IPsec) 578
protocol (Manual Security Association) 578
protocol (IP Headers in Signature Attack) 579
protocol (Signature Attack) 580
protocol-binding 583
protocol-command 584
protocol-name 584
protocols 585
protocols (Interface Host-Inbound Traffic) 586
protocols (Zone Host-Inbound Traffic) 588
proxy-arp 589
proxy-identity 589
raise-threshold 590
rate-limit 590
real 591
re-assembler 592
re-enroll-trigger-time-percentage 592
recommended 593
recommended-action 594
regexp 594
reject 595
reject-timeout 595
remote 596
remote-exceptions 596
remote-protected-resources 597
remove-r6 597
reset 598
reset-on-policy 598
respond-bad-spi 599
retain-hold-resource 599

revocation-check 600
route-change-timeout 600
routing-instance 601
routing-instance (Destination NAT) 601
routing-instance (Source NAT) 601
rpc 602
rsh 603
rst-invalidate-session 604
rst-sequence-check 604
rtsp 605
rule 606
rule (AppDDoS Rulebase) 606
rule (Destination NAT) 607
rule (Exempt Rulebase) 608
rule (IPS Rulebase) 609
rule (Source NAT) 610
rule (Static NAT) 611
rulebase-ddos 612
rule-set 613
rule-set (Destination NAT) 613
rule-set (Source NAT) 614
rule-set (Static NAT) 615
rulebase-exempt 616
rulebase-ips 617
sbl 618
sbl-default-server 619
scan-mode 619
scan-options 620
scan-options (antivirus juniper-express-engine) 620
scan-options (anti-virus kaspersky-lab-engine) 621
sccp 622
scheduler-name 623
scope 624
scope (Chain Attack) 624
scope (Custom Attack) 625
screen 626
screen (Security) 627
screen (Zones) 628
security-package 629
security-zone 630
sensor-configuration 631
seq-number-validated 632
server 633
server-connectivity 633
sessions 634
session-close 634
session-init 635
sessions-per-client 635
sequence-number 636
sequence-number (ICMP Headers in Signature Attack) 636
sequence-number (TCP Headers in Signature Attack) 637

service 638
service (AppDDoS) 638
service (Anomaly Attack) 638
service (Dynamic Attack Group) 639
service (Security IPsec) 639
severity 640
severity (Custom Attack) 640
severity (Dynamic Attack Group) 641
severity (IPS Rulebase) 642
shellcode 643
signature 644
sip 648
smtp-profile 649
smtp-profile (antispam utm-policy) 649
smtp-profile (antivirus utm-policy) 649
smtp-profile (content-filtering utm-policy) 650
sockets 650
source 651
source (IP Headers in Signature Attack) 651
source (Source NAT) 652
source-address 654
source-address (Destination NAT) 654
source-address (IDP Policy) 654
source-address (Source NAT) 655
source-address (Security Policies) 655
source-except 656
source-interface 656
source-ip-based 657
source-nat 658
source-port 659
source-threshold 660
spam-action 660
spi 661
sql 662
ssh-known-hosts 663
ssl-inspection 664
start-log 664
start-time 665
static 665
static-nat 666
strict-syn-check 666
sunrpc 667
suppression 668
surf-control-integrated 669
syn-ack-ack-proxy 670
syn-fin 670
syn-flood 671
syn-flood-protection-mode 672
syn-frag 672

system-services 673
system-services (Interface Host-Inbound Traffic) 674
system-services (Zone Host-Inbound Traffic) 676
t1-interval 677
t4-interval 678
talk 679
target 680
tcp 681
tcp (Protocol Binding Custom Attack) 681
tcp (Security Screen) 682
tcp (Signature Attack) 683
tcp-flags 685
tcp-initial-timeout 686
tcp-mss 687
tcp-no-flag 688
tcp-rst 688
tcp-session 689
terminal 689
test 690
tftp 691
then 692
then (Destination NAT) 692
then (IDP Policy) 693
then (rulebase-ddos) 694
then (Security Policies) 695
then (Source NAT) 696
then (Static NAT) 696
threshold 697
time-binding 697
time-binding-count 698
time-binding-period statement 699
timeout 700
timeout (GTP) 700
timeout (IDP Policy) 700
timeout (Security Screen) 701
timeout (utm) 702
timeout (antivirus fallback-options) 702
timeout (antivirus scan-options) 703
timeout (antivirus trickling) 703
timeout (web-filtering surf-control-integrated cache) 704
timeout (web-filtering fallback-settings) 704
timeout (web-filtering websense-redirect profile) 705
to 705
to-zone 706
too-many-requests 707
too-many-requests (antivirus fallback-options) 707
too-many-requests (web-filtering fallback-settings) 708
tos 709
total-length 710

traceoptions 711
traceoptions (firewall-authentication) 712
traceoptions (H.323 ALG) 713
traceoptions (Flow) 714
traceoptions (firewall-authentication) 716
traceoptions (IDP) 717
traceoptions (IKE) 719
traceoptions (IPsec) 720
traceoptions (MGCP ALG) 721
traceoptions (NAT) 722
traceoptions (datapath-debug) 724
traceoptions (PKI) 725
traceoptions (Policies) 727
traceoptions (SCCP ALG) 729
traceoptions (Screen) 730
traceoptions (Security) 732
traceoptions (SIP ALG) 734
traffic-options 735
transaction-timeout 735
trickling 736
trusted-ca 736
ttl 737
tunable-name 737
tunable-value 738
tunnel 738
type 739
type (ICMP Headers in Signature Attack) 739
type (Dynamic Attack Group) 739
type (utm) 740
type (antivirus fallback-block) 740
type (antivirus notification-options virus-detection) 741
type (content-filtering notification-options) 741
udp 742
udp (Protocol Binding Custom Attack) 742
udp (Security Screen) 743
udp (Signature Attack) 744
unknown-message 745
unknown-message (H.323 ALG) 745
unknown-message (MGCP ALG) 746
unknown-message (SCCP ALG) 747
unknown-message (SIP ALG) 748
upload-profile 749
upload-profile (ftp antivirus utm-profile) 749
upload-profile (ftp content-filtering utm-profile) 749
urgent-pointer 750
url 750
url (antivirus) 751
url (kaspersky-lab-engine) 751
url (juniper-express-engine) 751
url-blacklist 752

url-pattern 752
url-whitelist 753
    url-whitelist (antivirus) 753
    url-whitelist (web-filtering) 753
user 754
user-at-hostname 754
utm 755
utm-policy 760
value-hit-rate-threshold 761
virus-detection 762
vpn 763
vpn-monitor 764
vpn-monitor-options 765
web-authentication 766
web-redirect 767
weight 767
wildcard 768
window-scale 768
window-size 769
winnuke 769
xauth 770
zones 771

Chapter 19 Services Hierarchy and Statements 773

Services Configuration Statement Hierarchy 773
address 775
address (peer call server) 775
analog (station-type) 776
analog-template 777
auth-id (peer-call-server) 778
auth-id (station) 779
auth-password (peer-call-server) 780
auth-password (station) 781
auto-attendant 782
ca-profile 783
caller-id-transmit (analog template, sip-template) 784
call-type (policy) 785
call-type (route pattern) 787
cas-group 789
class-of-restriction 791
class-of-restriction (station) 792
class-of-restriction (analog template, sip template) 793
codec (peer call server) 794
codec (sip template) 795
description (peer call server) 795
description (trunk groups) 796
dial-plan (media gateway) 797
dial-plan (survivable call server) 798
digit-manipulation 799

digit-transform (rule) 800
digit-transform (trunk group) 800
direct-inward-dialing 801
direct-inward-line 801
directory 802
dtmf-method (peer call server, sip template) 803
extension (live-attendant) 804
extension-inherit 805
extension-number (voicemail) 806
extension (station) 807
features 808
format 809
from (route-policy) 809
heartbeat-normal-interval 810
heartbeat-survivable-interval 810
hours 811
guest 812
infranet-controller 813
interface 814
interval 815
live-attendant 816
media-gateway 817
monitor-timeout 818
music-on-hold 819
next hop (route policy) 819
order 820
password 820
peer call server (definition) 821
peer call server (media gateway) 822
peer-proxy-server 822
peer call server (route policy) 823
permission 823
policy 824
port 825
port (peer-call-server, media-gateway, survivable-call-service) 825
protocol (peer-call-server, media-gateway, survivable-call-service) 826
pstn-access-number 827
registration-expiry-timeout 827
regular-expression 828
response-threshold 828
ring-count 829
route pattern (dial plan) 830
route (route policy) 831
route-policy 832
server-certificate-subject 833
service-point (survivable call server, media gateway) 833
sip (media gateway, peer call server, survivable call server) 834
sip-template (sip) 835
sip-timeout 836
station 837
station-template 838

station-type 838
survivable-call-service 839
tdm-interface (analog station) 840
tdm-interface (direct-inward-line) 840
template (analog) 841
template (sip) 841
term (route policy) 842
then 842
test-only-mode 843
timeout 844
timeout-action 845
traceoptions 846
transport (survivable-call-service, media-gateway, peer-call-server) 847
trunk 848
trunk-group (definition) 849
trunk-group (route-pattern, route-policy) 850
unified-access-control 852
voice-activity-detection 853
voicemail 854
zone (media-gateway, survivable-call-service) 855

Chapter 20 SNMP Hierarchy and Statements 857

SNMP Configuration Statement Hierarchy 857
authorization 862
client-list-name 862

Chapter 21 System Hierarchy and Statements 863

System Configuration Statement Hierarchy 863
firewall-authentication-service 873
general-authentication-service 874
network-security 875
pki-local-certificate 875
Port 876
    port (reverse ssh) 876
    port (reverse telnet) 876
propagate-settings 877
reverse ssh 877
reverse telnet 878
system-generated-certificate 878
traceoptions 879
    traceoptions (General Authentication Service) 880
    traceoptions (WAN Acceleration) 882
wan-acceleration 883

Chapter 22 Wlan Hierarchy and Statements 885

[edit wlan] Configuration Statement Hierarchy 885
access-point 889
access-point-options 893
access-point-queues 894
arbitration-inter-frame-space 895
background-queue 895
beacon-interval 896
best-effort-queue 896
broadcast-multicast-rate-limit 897
channel 897
console 898
country 899
disable-dot11d 900
dot1x 901
dot1x-supplicant 902
dtim-period 902
external 903
fixed-multicast-rate 904
fragmentation-threshold 904
ethernet 905
http-redirect 905
mac-authentication-type 906
management-vlan 906
maximum-stations 907
maximum-burst 907
maximum-contention-window 908
minimum-contention-window 908
mode 909
name-server 909
no-acknowledgement 910
no-auto-power-save 910
no-broadcast-ssid 911
no-short-guard-interval-supported 911
no-wifi-multimedia 911
ntp-server 912
protection 912
quality-of-service 913
radio 915
radio-off 917
radio-options 918
rts-threshold 919
security 920
space-time-block-coding 921
ssid 921
static 921
static-wep 922
station-mac-filter 923

station-queues 924
transmit-opportunity-limit 925
transmit-power 925
transmit-rate-sets 926
untagged-vlan 926
video-queue 927
virtual-access-point 928
vlan 929
voice-queue 930
wpa-enterprise 931
wpa-personal 932

Part 2 Operational Commands

Chapter 23 Clear Commands 935

clear chassis cluster control-plane statistics 936
clear chassis cluster data-plane statistics 937
clear chassis cluster failover-count 938
clear chassis cluster statistics 939
clear esis adjacency 940
clear esis statistics 941
clear network-access requests pending 942
clear gtp tunnels 943
clear network-access requests statistics 944
clear network-access securid-node-secret-file 945
clear security alg h323 counters 946
clear security alg mgcp calls 947
clear security alg mgcp counters 948
clear security alg msrpc portmap 949
clear security alg sccp calls 950
clear security alg sccp counters 951
clear security alg sip calls 952
clear security alg sip counters 953
clear security alg sunrpc portmap 954
clear security alg sunrpc portmap 955
clear security datapath-debug counter 956
clear security firewall-authentication history 957
clear security firewall-authentication history address 958
clear security firewall-authentication history identifier 959
clear security firewall-authentication users 960
clear security firewall-authentication users address 961
clear security firewall-authentication users identifier 962
clear security flow session all 963
clear security flow session application 964
clear security flow session destination-port 966
clear security flow session destination-prefix 967
clear security flow session interface 968

clear security flow session protocol 969
clear security flow session resource-manager 971
clear security flow session session-identifier 972
clear security flow session source-port 973
clear security flow session source-prefix 974
clear security idp application-identification application-system-cache 975
clear security idp attack table 976
clear security idp counters application-identification 977
clear security idp counters dfa 978
clear security idp counters flow 979
clear security idp counters ips 980
clear security idp counters log 981
clear security idp counters packet 982
clear security idp counters policy-manager 983
clear security idp counters tcp-reassembler 984
clear security idp ssl-inspection session-id-cache 985
clear security ike respond-bad-spi-count 986
clear security ike security-associations 987
clear security ipsec security-associations 989
clear security ipsec statistics 990
clear security nat incoming-table 991
clear security nat source persistent-nat-table 992
clear security pki key-pair 993
clear security pki local-certificate 994
clear security policies statistics 995
clear security screen statistics 996
clear security screen statistics interface 997
clear security screen statistics zone 998
clear security utm anti-spam statistics 999
clear security utm antivirus statistics 1000
clear security utm content-filtering statistics 1001
clear security utm session 1002
clear security utm web-filtering statistics 1003

Chapter 24 Request Commands 1005

request chassis cluster failover node 1006
request chassis cluster failover reset 1007
request modem wireless activate iota 1008
request modem wireless activate manual 1009
request modem wireless activate otasp 1011
request modem wireless gsm sim-unblock 1012
request modem wireless gsm sim-unlock 1013
request security datapath-debug capture start 1014
request security datapath-debug capture stop 1015
request security idp security-package download 1016
request security idp security-package install 1018
request security idp ssl-inspection key add 1019
request security idp ssl-inspection key delete 1021
request security pki ca-certificate verify 1022

request security pki local-certificate generate-self-signed 1023
request security pki local-certificate verify 1025
request security utm anti-virus juniper-express-engine 1026
request security utm anti-virus kaspersky-lab-engine 1027
request system license update 1028
request system partition compact-flash 1029
request system services dhcp 1030
request system software in-service-upgrade 1031
request wan-acceleration login 1033
request wlan access-point firmware upgrade 1034
request wlan access-point restart 1035

Chapter 25 Restart Commands 1037

restart 1038

Chapter 26 Show Commands 1039

show bgp neighbor 1040
show chassis cluster control-plane statistics 1044
show chassis cluster data-plane statistics 1046
show chassis cluster interfaces 1048
show chassis cluster ip-monitoring status redundancy-group 1050
show chassis cluster statistics 1052
show chassis cluster status 1056
show chassis fpc 1059
show chassis hardware 1062
show esis adjacency 1067
show esis interface 1069
show esis statistics 1071
show ethernet-switching mac-learning-log 1072
show ethernet-switching table 1074
show gtp tunnels 1078
show igmp-snooping route 1079
show igmp-snooping vlans 1081
show interfaces 1083
show interfaces flow-statistics 1089
show modem wireless interface 1091
show modem wireless interface firmware 1093
show modem wireless interface network 1095
show modem wireless interface rssi 1097
show network-access requests pending 1098
show network-access requests statistics 1100
show network-access securid-node-secret-file 1101
show poe controller 1102
show poe interface 1103
show poe telemetries interface 1105
show schedulers 1107
show security alg h323 counters 1109
show security alg mgcp calls 1111

show security alg mgcp counters 1113
show security alg mgcp endpoints 1115
show security alg msrpc 1117
show security alg sccp calls 1119
show security alg sccp counters 1121
show security alg sip calls 1123
show security alg sip counters 1126
show security alg sip rate 1130
show security alg sip transactions 1131
show security alg status 1132
show security alg sunrpc portmap 1134
show security datapath-debug capture 1135
show security datapath-debug capture 1136
show security datapath-debug counter 1137
show security dynamic-vpn client version 1138
show security dynamic-vpn users 1139
show security dynamic-vpn users terse 1140
show security firewall-authentication history 1141
show security firewall-authentication history address 1143
show security firewall-authentication history identifier 1146
show security firewall-authentication users 1148
show security firewall-authentication users address 1150
show security firewall-authentication users identifier 1152
show security flow gate 1154
show security flow session 1157
show security flow session application 1159
show security flow session destination-port 1161
show security flow session destination-prefix 1163
show security flow session interface 1165
show security flow session protocol 1167
show security flow session resource-manager 1170
show security flow session session-identifier 1172
show security flow session source-port 1176
show security flow session source-prefix 1178
show security flow session summary 1180
show security flow session tunnel 1182
show security idp active-policy 1184
show security idp application-ddos application 1185
show security idp application-identification application-system-cache 1187
show security idp attack table 1188
show security idp counters application-ddos 1189
show security idp counters application-identification 1191
show security idp counters dfa 1193
show security idp counters flow 1194
show security idp counters ips 1197
show security idp counters log 1199
show security idp counters packet 1202
show security idp counters policy-manager 1205
show security idp counters tcp-reassembler 1206
show security idp memory 1209
show security idp security-package-version 1210

show security idp ssl-inspection key 1211
show security idp ssl-inspection session-id-cache 1212
show security idp status 1213
show security ike pre-shared-key 1214
show security ike security-associations 1215
show security ipsec next-hop-tunnels 1220
show security ipsec security-associations 1221
show security ipsec statistics 1227
show security monitoring fpc fpc-number 1230
show security nat destination pool 1232
show security nat destination rule 1234
show security nat destination summary 1237
show security nat incoming-table 1239
show security nat interface-nat-ports 1241
show security nat source persistent-nat-table 1243
show security nat source pool 1245
show security nat source rule 1247
show security nat source summary 1250
show security nat static rule 1252
show security nat static-nat summary 1254
show security pki ca-certificate 1256
show security pki certificate-request 1260
show security pki crl 1262
show security pki local-certificate 1264
show security policies 1268
show security resource-manager group active 1271
show security resource-manager resource active 1273
show security resource-manager settings 1275
show security screen ids-option 1277
show security screen statistics 1279
show security utm anti-spam statistics 1284
show security utm anti-spam status 1285
show security utm anti-virus statistics 1286
show security utm anti-virus status 1287
show security utm content-filtering statistics 1288
show security utm session 1289
show security utm status 1290
show security utm web-filtering statistics 1291
show security utm web-filtering status 1292
show security zones 1293
show security zones type 1295
show services unified-access-control authentication-table 1297
show services unified-access-control policies 1298
show services unified-access-control status 1299
show system services dhcp client 1300
show system services dhcp relay-statistics 1303
show wan-acceleration status 1305
show wlan access-points 1306

Part 3 Index

Index 1311

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software CLI Reference*:

- J Series and SRX Series Documentation and Release Notes on page xxxvii
- Objectives on page xxxviii
- Audience on page xxxviii
- Supported Routing Platforms on page xxxviii
- How to Use This Manual on page xxxviii
- 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 Software 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 JUNOS Software 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 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 .

Objectives

This reference documents command-line interface (CLI) statements and commands for J Series Services Routers and SRX Series Services Gateways running JUNOS Software. 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 Software—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 Software. 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 Software.

How to Use This Manual

This manual and the other manuals in this set explain how to install, configure, and manage:

- JUNOS Software for J Series Services Routers
- JUNOS Software for SRX Series Services Gateways

Table 1 on page xxxix identifies the tasks required to configure and manage these devices and shows where to find task information and instructions.

Table 1: Tasks and Related Documentation

Task	Related Documentation
Basic Device Installation and Setup	
■ Reviewing safety warnings and compliance statements ■ Installing hardware and establishing basic connectivity ■ Initially setting up a device	J Series Services Routers: ■ *J Series Services Routers Quick Start* ■ *J Series Services Routers Hardware Guide* ■ *JUNOS Software Release Notes* SRX Series Services Gateways: the appropriate *Services Gateway Getting Started Guide*
Migration from ScreenOS or JUNOS Software (Legacy Services) to JUNOS Software (if necessary)	
■ Migrating from JUNOS Software (legacy services) Release 8.3 or later to JUNOS Software ■ Migrating from ScreenOS Release 5.4 or later to JUNOS Software.	*JUNOS Software Migration Guide* (J Series Services Routers only)
Context—Changing to Secure Context or Router Context	
Changing the device from one context to another and understanding the factory default settings	*JUNOS Software Administration Guide*
Interface Configuration	
Configuring device interfaces	■ *JUNOS Software Interfaces and Routing Configuration Guide* ■ *JUNOS Software CLI Reference*
Deployment Planning and Configuration	
■ Understanding and gathering information required to design network firewalls and IPsec VPNs ■ Implementing a JUNOS Software firewall from a sample scenario ■ Implementing a policy-based IPsec VPN from a sample scenario	*JUNOS Software Design and Implementation Guide* (J Series Services Routers only)
Security Configuration	
Configuring and managing the following security services: ■ Stateful firewall policies ■ Zones and their interfaces and address books ■ IPsec VPNs ■ Firewall screens ■ Interface modes: Network Address Translation (NAT) mode and Router mode ■ Public Key Cryptography (PKI) ■ Application Layer Gateways (ALGs) ■ Chassis clusters ■ Intrusion Detection and Prevention (IDP)	■ *JUNOS Software Security Configuration Guide* ■ *JUNOS Software CLI Reference*
Routing Protocols and Services Configuration	

Table 1: Tasks and Related Documentation *(continued)*

Task	Related Documentation
■ Configuring routing protocols, including static routes and the dynamic routing protocols RIP, OSPF, BGP, and IS-IS ■ Configuring class-of-service (CoS) features, including traffic shaping and policing ■ Configuring packet-based stateless firewall filters (access control lists) to control access and limit traffic rates ■ Configuring MPLS to control network traffic patterns	■ *JUNOS Software Interfaces and Routing Configuration Guide* ■ *JUNOS Software CLI Reference*
WAN Acceleration Module Installation (Optional)	
Installing and initially configuring a WXC Integrated Services Module (ISM 200)	*WXC Integrated Services Module Installation and Configuration Guide* (J Series Services Routers only)
User and System Administration	
■ Administering user authentication and access ■ Monitoring the device, routing protocols, and routing operations ■ Configuring and monitoring system alarms and events, real-time performance (RPM) probes, and performance ■ Monitoring the firewall and other security-related services ■ Managing system log files ■ Upgrading software ■ Diagnosing common problems	*JUNOS Software Administration Guide*
User Interfaces	
■ Understanding and using the J-Web interface ■ Understanding and using the CLI configuration editor	■ *J Series Services Routers Quick Start* (J Series Services Routers only) ■ *JUNOS Software Administration Guide*

Document Conventions

Table 2 on page xli defines the notice icons used in this guide.

Table 2: 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 3 on page xli defines the text and syntax conventions used in this guide.

Table 3: 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 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*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; 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 3: 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, 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/customers/support/downloads/710059.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/
- Search for known bugs: http://www2.juniper.net/kb/
- 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

Part 1
Configuration Statements

- Access Hierarchy and Statements on page 3
- Accounting-Options Hierarchy on page 37
- Applications Hierarchy and Statements on page 39
- Bridge-Domains Hierarchy and Statements on page 53
- Chassis Hierarchy and Statements on page 59
- Class-of-Service Hierarchy and Statements on page 79
- Event-Options Hierarchy on page 101
- Firewall Hierarchy and Statements on page 103
- Forwarding-Options Hierarchy and Statements on page 109
- Groups Hierarchy on page 115
- Interfaces Hierarchy and Statements on page 117
- Power Over Ethernet Hierarchy and Statements on page 157
- Policy-Options Hierarchy and Statements on page 165
- Protocols Hierarchy and Statements on page 169
- Routing-Instances Hierarchy on page 201
- Routing-Options Hierarchy on page 213
- Schedulers Hierarchy and Statements on page 221
- Security Hierarchy and Statements on page 237
- Services Hierarchy and Statements on page 773
- SNMP Hierarchy and Statements on page 857
- System Hierarchy and Statements on page 863
- Wlan Hierarchy and Statements on page 885

Chapter 1

Access Hierarchy and Statements

This chapter presents the complete access configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the access configuration hierarchy to configure access to the device and user authentication methods. For configuration instructions, see the *JUNOS Software Security Configuration Guide*.

For information about access statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS System Basics Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

■ Access Configuration Statement Hierarchy on page 3

Access Configuration Statement Hierarchy

To configure device access and user authentication, use the following statements at the [edit access] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the access hierarchy are shown in normal font and are documented in the *JUNOS System Basics Configuration Guide*.

```
access {
    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;
    }
}
access {
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;
    }
}
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;
}
profile  profile-name {
    accounting-order [ accounting-methods];
    authentication-order (ldap | password | radius | securid);
    client  client-name {
        chap-secret  chap-secret;
        client-group [ group-names ];
        firewall-user {
            password password;
        }
        pap-password  pap-password;
    }
    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;
    }
```

```
    }
    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;
    }
}
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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."

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

authentication-order

Syntax authentication-order (ldap | password | radius | securid);

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

Release Information Statement modified in Release 9.1 of JUNOS Software.

Description Set the order in which the JUNOS Software 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

banner

See the following sections:

- banner (FTP, HTTP, Telnet) on page 8
- banner (Web Authentication) on page 9

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specifies 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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 10000 minutes
Default: Off

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

configuration-file

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

Hierarchy Level [edit access securid-server]

Release Information Statement introduced in Release 9.1 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 (" ").

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure LDAP authentication options.

Options The remaining options are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines
For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 (" ").

Usage Guidelines
For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

port

See the following sections:

- port (LDAP) on page 22
- port (RADIUS) on page 22

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description
Configure RADIUS options.

Options
The remaining statement is explained separately.

Usage Guidelines
For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

retry

See the following sections:

- retry (LDAP) on page 25
- retry (RADIUS) on page 25

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*. See also timeout.

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

revert-interval

See the following sections:

- revert-interval (LDAP) on page 26
- revert-interval (RADIUS) on page 26

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 Software.

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 4294967295 seconds
Default: 600 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

revert-interval (RADIUS)

Syntax revert-interval *seconds*;

Hierarchy Level [edit access radius-options]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 4294967295 seconds
Default: 600 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

routing-instance

See the following sections:

- routing-instance (LDAP) on page 27
- routing-instance (RADIUS) on page 27

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

securid-server

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

Hierarchy Level [edit access]

Release Information Statement introduced in Release 9.1 of JUNOS Software.

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 supported for this release.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

source-address

See the following sections:

- source-address (LDAP) on page 31
- source-address (RADIUS) on page 31

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 Software.

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 IPv4 address configured on one of the device interfaces.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 IPv4 address configured on one of the device interfaces.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 (" ").

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

timeout

See the following sections:

- timeout (LDAP Server) on page 33
- timeout (RADIUS Server) on page 33

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 2

Accounting-Options Hierarchy

This chapter presents the complete accounting-options configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

Use the statements in the accounting-options configuration hierarchy to collect and log data about basic system operations and services on the device. For configuration instructions, see the *JUNOS Software Administration Guide*.

For information about these accounting-options statements that are shared across Juniper Networks devices, see the *JUNOS Network Management Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Accounting-Options Configuration Statement Hierarchy on page 37

Accounting-Options Configuration Statement Hierarchy

To configure accounting options, use the following statements at the [edit accounting-options] hierarchy level.

Shared JUNOS statements in the accounting-options hierarchy are shown in normal font and are documented in the *JUNOS Network Management Configuration Guide*.

```
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 ;
    }
}
```

Chapter 3

Applications Hierarchy and Statements

This chapter presents the complete applications configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the applications configuration hierarchy to configure applications functions of J Series and SRX Series devices and their properties on the device. For configuration instructions, see the *JUNOS Software Security Configuration Guide*.

For information about applications statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS Services Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Applications Configuration Statement Hierarchy on page 39

Applications Configuration Statement Hierarchy

To configure applications properties and to group application objects, use the following statements at the [edit applications] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the applications hierarchy are shown in normal font and are documented in the *JUNOS Services Interfaces Configuration Guide*.

```
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 ];
  }
}
```

alg

Syntax alg *application* ;

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

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application-protocol

Syntax application-protocol *protocol-name* ;

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

Release Information Statement modified in Release 8.5 of JUNOS Software.

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
- 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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 4 on page 44.

Table 4: Port Names 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
kshell	544
ldap	389
ldp	646

Table 4: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
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
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs	49

Table 4: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
tacacs-ds	65
talk	517
telnet	23
tftp	69
timed	525
who	513
xdmcp	177

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the ICMP packet type value.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Inactivity timeout period, in seconds.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Options *number* —RPC or DCE program value.
Range: 0 through 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 4 on page 44.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define individual application protocols.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 portmap ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

Options *hex-value* —Hexadecimal value.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 4

Bridge-Domains Hierarchy and Statements

This chapter presents the complete bridge-domains configuration hierarchy available on SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to SRX Series devices. Statement summaries are organized alphabetically.

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. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Bridge-Domains Configuration Statement Hierarchy on page 53

Bridge-Domains Configuration Statement Hierarchy

To configure bridge domains, use the following statements at the [edit bridge-domains] hierarchy level. Statements exclusively for SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

```
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;
    }
}
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

domain-type

Syntax domain-type bridge;

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

Release Information Statement modified in Release 9.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

interface

Syntax interface *interface-name*;

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

Release Information Statement modified in Release 9.5 of JUNOS Software.

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

Options *interface-name*—Name of a logical interface. For more information about how to configure logical interfaces, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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. For more information about how to configure an IRB interface, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

Options *mac-address*—MAC address

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

Chapter 5

Chassis Hierarchy and Statements

This chapter presents the complete chassis configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. . Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the chassis configuration hierarchy to configure alarms and other chassis properties and to configure chassis clusters. For configuration instructions, see the *J Series Services Routers Hardware Guide* and the *JUNOS Software Administration Guide*. To configure chassis clusters, see the *JUNOS Software Security Configuration Guide*.

For information about chassis statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS System Basics Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Chassis Configuration Statement Hierarchy on page 59

Chassis Configuration Statement Hierarchy

To configure chassis properties, use the following statements at the [edit chassis] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the chassis hierarchy are shown in normal font and are documented in the *JUNOS System Basics Configuration Guide*.

```
chassis {
    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);
        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 {
            weight number threshold number ;
            family {
                inet {
                    IPv4 address weight number
```

```
            }
          }
        }
        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;
        }
      }
}
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 ;
                }
            }
        }
        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;
          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);
      }
      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);
      }
    }
```

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 {
            weight number threshold number ;
            family {
                inet {
                    IPv4 address weight number
                }
            }
        }
        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 Software.

Description Configure a chassis cluster.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

control-link-recovery

Syntax control-link-recovery;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software. Support for dual control ports added in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

heartbeat-interval

Syntax heartbeat-interval *milliseconds* ;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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

Options *milliseconds* —Time interval between any two heartbeat messages.
Range: 1000 through 2000 milliseconds
Default: 1000 milliseconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

heartbeat-threshold

Syntax heartbeat-threshold *number* ;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Options *number* —Number of consecutive missed heartbeats.
Range: 3 through 8
Default: 3

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ip-monitoring

Syntax

```
ip-monitoring {
   weight number threshold number ;
   family {
         inet {
            IPv4 address weight number
         }
   }
}
```

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

Release Information Statement introduced in Release 9.6 of JUNOS Software.

Description Specify an IP address monitoring threshold and weight and IP addresses for the redundancy group interface to monitor.

Options *IPv4–address* —The address to be continually monitored for reachability.

NOTE: All monitored object failures, including IP monitoring, are deducted from the 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

node

See the following sections:

- node (Cluster) on page 70
- node (Redundancy-Group) on page 70

node (Cluster)

Syntax node *node-number* ;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

preempt

Syntax preempt;

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

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

redundancy-group

Syntax

```
redundancy-group group-number {
  gratuitous-arp-count number ;
  hold-down-interval number ;
  interface-monitor interface {
    weight number ;
  }
  ip-monitoring {
    weight number threshold number ;
    family {
        inet {
          IPv4 address weight number
        }
    }
  }
  node node-number {
    priority priority-number ;
  }
  preempt;
}
```

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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 (reth) interface.

Redundancy group 0 consists of the two Routing Engines in the chassis cluster and controls Routing Engine primaryship. 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

reth-count

Syntax reth-count *number* ;

Hierarchy Level [edit chassis cluster]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

threshold

Syntax threshold *number* ;

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

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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 will be 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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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]

Release Information Statement modified in Release 9.6 of JUNOS Software.

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. If the object, or in the case of IP monitoring enough monitored addresses, fails, the weight of the object is deducted from the threshold of its 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* —Weight assigned to the interface. A higher weight value indicates a greater importance.
Range: 0 through 255

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 6

Class-of-Service Hierarchy and Statements

This chapter presents the complete class-of-service configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the class-of-service configuration hierarchy to configure class-of-services (CoS) features. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following section:

- Class-of-Service Configuration Statement Hierarchy on page 79

Class-of-Service Configuration Statement Hierarchy

To configure CoS, use the following statements at the [edit class-of-service] hierarchy level.

```
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-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 ;
      }
    }
}
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 | 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) <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 ;
    }
}
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics adaptive-shapers

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics adaptive-shaper

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics scheduler-map (Virtual Channels), shaping-rate (Virtual Channels), virtual-channel-group, virtual-channel-groups, virtual-channels

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.
ieee-802.1ad option introduced in 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics rewrite-rules (Interfaces)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics rewrite-rules (Definition)

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 Software.

Description Apply a scheduler map to this virtual channel.

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

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics default, shaping-rate (Virtual Channels), virtual-channel-group, virtual-channel-groups, virtual-channels

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics trigger

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 Software.

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 Software Interfaces and Routing Guide*.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics default, scheduler-map (Virtual Channels), virtual-channel-group, virtual-channel-groups, virtual-channels

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 Software.

Description Specify a trigger type and its associated rate.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics shaping-rate (Adaptive Shaping)

virtual-channels

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

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify a list of virtual channels.

Each virtual channel has eight transmission queues.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics default, scheduler-map (Virtual Channels), shaping-rate (Virtual Channels), virtual-channel-group, virtual-channel-groups.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics default, scheduler-map (Virtual Channels), shaping-rate (Virtual Channels), virtual-channels, virtual-channel-groups.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Guide*.

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

Related Topics default, scheduler-map (Virtual Channels), shaping-rate (Virtual Channels), virtual-channel-group, virtual-channels.

Chapter 7

Event-Options Hierarchy

This chapter presents the complete event-options configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

Use the statements in the event-options configuration hierarchy to configure diagnostic event policies and actions associated with each policy. For configuration instructions, see the *JUNOS Software Administration Guide*.

For information about these event-options statements that are shared across Juniper Networks devices, see the *JUNOS Configuration and Diagnostic Automation Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Event-Options Configuration Statement Hierarchy on page 101

Event-Options Configuration Statement Hierarchy

To configure event policies, use the following statements at the [edit event-options] hierarchy level.

Shared JUNOS statements in the event-options hierarchy are shown in normal font and are documented in the *JUNOS Configuration and Diagnostic Automation Guide*.

```
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 ;
}
}
```

Chapter 8

Firewall Hierarchy and Statements

This chapter presents the complete firewall configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the firewall configuration hierarchy to configure stateless firewall filters—also known as access control lists (ACLs)—on the device. Stateless firewall filters allow you to filter packets based on their components and to perform an action on packets that match the filter. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about these firewall statements that are shared across Juniper Networks devices—see the *JUNOS Policy Framework Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Firewall Configuration Statement Hierarchy on page 103

Firewall Configuration Statement Hierarchy

To configure stateless firewall filters, use the following statements at the [edit firewall] hierarchy level.

Shared JUNOS statements in the firewall hierarchy are shown in normal font and are documented in the *JUNOS Policy Framework Configuration Guide*.

```
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  {
    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 ;
    }
}
```

```
}
```

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 Software.

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.

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 inet filter *filter-name*]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Chapter 9

Forwarding-Options Hierarchy and Statements

This chapter presents the complete forwarding-options configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the forwarding-options configuration hierarchy to configure forwarding options protocols, including flow monitoring. accounting properties, and packet capture. For configuration instructions, see the *JUNOS Software Administration Guide*.

For information about these forwarding-options statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS Policy Options Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Forwarding-Options Configuration Statement Hierarchy on page 109

Forwarding-Options Configuration Statement Hierarchy

To configure forwarding options, use the following statements at the [edit forwarding-options] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the forwarding-options hierarchy are shown in normal font and are documented in the *JUNOS Policy Options Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

```
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;
         }
         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 {
    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>;
        }
    }
}
```

vpn

Syntax vpn;

Hierarchy Level [edit forwarding-options helpers bootp]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Usage Guidelines To configure DHCP, see the *JUNOS Software Administration Guide*.

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

Chapter 10
Groups Hierarchy

This chapter presents the complete groups configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Use the statements in the groups configuration hierarchy to configure information that can be dynamically updated in different parts of the device configuration.

For information about these groups statements that are shared across Juniper Networks devices, see the *JUNOS CLI User Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Groups Configuration Statement Hierarchy on page 115

Groups Configuration Statement Hierarchy

To configure groups, use the following statements at the [edit groups] hierarchy level.

Shared JUNOS statements in the groups hierarchy are shown in normal font and are documented in the *JUNOS CLI User Guide*.

```
groups {
    group-name  {
        configuration-data ;
    }
}
```

Chapter 11

Interfaces Hierarchy and Statements

This chapter presents the complete interfaces configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the interfaces configuration hierarchy to configure interfaces on the device. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide* and the *JUNOS Software Administration Guide*.

For information about interfaces statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Interfaces Configuration Statement Hierarchy on page 117

Interfaces Configuration Statement Hierarchy

To configure interfaces, use the following statements at the [edit interfaces] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the interfaces hierarchy are shown in normal font and are documented in the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

```
interfaces {
    interface-name  {
        accounting-profile  name ;
        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);
}
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 {
    (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 {
    calling-number number ;
    incoming-called-number number <reject>;
    pool pool-name <priority priority> ;
    spid1 spid-string ;
    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 ;
}
redundant-ether-options {
    (flow-control | no-flow-control);
    link-speed speed;
    (loopback | no-loopback);
    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 ;
    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 ;
}
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 ;
    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 ;
(atm-cisco-nlpid | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux |
    atm-snap | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc |
    ppp-over-ether | ppp-over-ether-over-atm-llc)
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
      }
    }
}
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 ;
  }
  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);
    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>;
      }
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 JUNOS Release 8.2.

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 Topics *JUNOS Software Interfaces and Routing Configuration Guide*

annex

Syntax annex *annex-type*

Hierarchy Level [edit interfaces *interfaces-name* shdsl-options]

Release Information Command introduced in Release 10.0 of JUNOS Software.

Description Select an annex type that suits your requirements for configuring G.SHDSL interface.

Options
- Annex A
- Annex B
- Annex F
- Annex G

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 JUNOS Release 8.2.

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 Topics *JUNOS Software Interfaces and Routing Configuration Guide*

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 Software.

Description Specify the logical interface name the link joins.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description For ATM encapsulation only, define a constant bit rate bandwidth utilization in the traffic-shaping profile.

Options CBR Value - Constant bandwidth utilization (range: (33000 – 1199920)

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.

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 Software.

Description Configure options for connecting a 3G wireless modem interface to a cellular network.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

client-identifier

Syntax client-identifier (ascii *ascii* | hexadecimal *hexadecimal*);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

compression-device

Syntax compression-device *name*;

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

Release Information Statement introduced before JUNOS Release 7.4.

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 Topics *JUNOS Software Interfaces and Routing Configuration Guide*

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 Software.

Description Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options The statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

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 JUNOS Release 8.2.

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 Topics *JUNOS Software Interfaces and Routing Configuration Guide*

encapsulation

Syntax encapsulation
(atm-cisco-nlpid | **atm-mlppp-llc** | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | **ppp-over-ether** | **ppp-over-ether-over-atm-llc**)

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

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Specifies logical link layer encapsulation.

atm-mlppp-llc—Configure MLPPP over AAL5/LLC.

ppp-over-ether—For underlying Ethernet interfaces on J Series devices only, use PPP over Ethernet encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, you configure the interface address on the PPP interface. For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

ppp-over-ether-over-atm-llc—For underlying ATM interfaces on J Series devices only, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, you configure the interface address on the PPP interface. For more information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure fabric interface properties.

Options The remaining statement is explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

fpc

Syntax fpc;

Hierarchy Level [edit interfaces pic-set pic-set-name]

Release Information Command introduced in Release 9.6 of JUNOS Software.

Description Sets the PIC bundle and the and the FPC slot.

Options *apply-groups*– Groups from which to inherit configuration data.

apply-groups-except– Do not inherit configuration data from these groups.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

lease-time

Syntax lease-time *seconds* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 2147483647 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

line-rate

Syntax line-rate

Hierarchy Level [edit interfaces *interfaces name* shdsl-options]

Release Information Command introduced in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description For redundant Ethernet interfaces (reth0) 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).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

loopback

Syntax (loopback | no-loopback);

Hierarchy Level [edit interfaces *interface-name* redundant-ether-options]

Release Information Statement modified in Release 9.0 of JUNOS Software.

Description For Fast Ethernet, Gigabit Ethernet, and redundant Ethernet interfaces, enable or disable loopback mode.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

native-vlan-id

Syntax native-vlan-id *vlan-id*;

Hierarchy Level [edit interfaces *interface*]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

next-hop-tunnel

Syntax next-hop-tunnel *gateway-address* ipsec-vpn *vpn-name* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

no-flow-control

See flow-control

no-loopback

See loopback

no-source-filtering

See source-filtering

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*. See also redundancy-group.

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

redundant-ether-options

Syntax
```
redundant-ether-options {
    (flow-control | no-flow-control);
    link-speed speed ;
    (loopback | no-loopback);
    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 Software.

Description Configure Ethernet redundancy options for a chassis cluster.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

redundant-parent

See the following sections:

- redundant-parent (Fast Ethernet Options) on page 148
- redundant-parent (Gigabit Ethernet Options) on page 148

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 Software.

Description Configure Fast Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

Options *interface* —Parent redundant interface of the Fast Ethernet interface.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure Gigabit Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

Options *interface* —Parent redundant interface of the Giganet Ethernet interface.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

retransmission-attempt

Syntax retransmission-attempt *number* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

retransmission-interval

Syntax retransmission-interval *seconds* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the time between successive retransmission attempts.

Options *seconds* —Number of seconds between successive retransmission.
Range: 4 through 64 seconds
Default: 4 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

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 Software.

Description Specifies 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

server-address

Syntax server-address *ip-address* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the preferred DHCP server address that is sent to DHCP clients.

Options *ip-address* —DHCP server address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

simple-filter

Syntax
```
simple-filter{
   input filter-name;
}
```

Hierarchy Level [edit interfaces *interfaces-name* unit *logical-unit-number* family inet]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Apply a simple filter to an interface. You can apply simple filters to the family inet only, and only in the input direction.

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.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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* (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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*. See also source-filtering.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*. See also source-address-filter.

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

update-server

Syntax update-server;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Propagate DHCP options to a local DHCP server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

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 Software.

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.

vendor-id

Syntax vendor-id *vendor-id* ;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

Options *vendor-id* —vendor class ID.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

web-authentication

Syntax
```
web-authentication {
    http;
}
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable the Web authentication process for firewall user authentication.

http—Enable HTTP service.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 12

Power Over Ethernet Hierarchy and Statements

This chapter presents the complete poe configuration hierarchy available on SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the poe configuration hierarchy to configure Power over Ethernet options. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- PoE Configuration Statement Hierarchy on page 157

PoE Configuration Statement Hierarchy

To configure Power over Ethernet options, use the following statements at the [edit poe] hierarchy level. Statements exclusively for SRX Series devices running JUNOS Software are shown in bold font and are documented 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;
        }
    }
}
```

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 Software.

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.

duration

Syntax duration hours;

Hierarchy Level [edit poe interface (all | interface-name) telemetries]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

guard-band

Syntax guard-band watts;

Hierarchy Level [edit poe]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

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 Software.

Description Enables 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— Applies the configuration to all interfaces on the SRX Series device that have not been explicitly configured otherwise.

interface-name— Explicitly configures 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.

interval

Syntax interval minutes;

Hierarchy Level [edit poe interface (all | interface-name) telemetries]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

management

Syntax management type;

Hierarchy Level [edit poe]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

maximum-power

Syntax maximum-power watts;

Hierarchy Level [edit poe interface (all | interface-name)]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

priority

Syntax priority value;

Hierarchy Level [edit poe interface (all | interface-name)]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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—Specifies that this port is to be treated as high priority in terms of power allocation

low—Specifies 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.

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 Software.

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 Topics

- Power Over Ethernet Hierarchy and Statements on page 157

Chapter 13

Policy-Options Hierarchy and Statements

This chapter presents the complete policy-options configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the policy-options configuration hierarchy to configure routing policies that control the information from routing protocols that the device imports into its routing table and exports to its neighbors. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about policy-options statements that are that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS Policy Framework Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Policy-Options Configuration Statement Hierarchy on page 165

Policy-Options Configuration Statement Hierarchy

To configure policy options, use the following statements at the [edit policy-options] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the policy-options hierarchy are shown in normal font and are documented in the *JUNOS Policy Framework Configuration Guide*.

```
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;
    }
}
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description For chassis cluster configurations, identify the device (node) on which a route is active.

Options node0 | node1—Node in a chassis cluster.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 14

Protocols Hierarchy and Statements

This chapter presents the complete protocols configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

Use the statements in the protocols configuration hierarchy 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), and Border Gateway Protocol (BGP), and Layer 2 address learning and forwarding properties. For configuration instructions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about these protocols statements that are shared across Juniper Networks devices, see the *JUNOS Routing Protocols Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Protocols Configuration Statement Hierarchy on page 169

Protocols Configuration Statement Hierarchy

To configure protocols, use the following statements at the [edit protocols] hierarchy level. Statements exclusively for SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the protocols hierarchy are shown in normal font and are documented in the *JUNOS Routing Protocols Configuration Guide*, the *JUNOS MPLS Applications Configuration Guide*, the *JUNOS Multicast Protocols Configuration Guide*, and the *JUNOS Services Interfaces Configuration Guide.*

```
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 ;
      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-nam e;
      transmit-lsp path-name ;
   }
   remote-interface-switch {
      interface interface-name ;
      receive-lsp path-nam e;
      transmit-lsp path-name ;
   }
}
dot1x {
   authenticator {
      authentication-profile-name profile-name ;
      interface interface-name {
         disable;
         guest-vlan vlan-name ;
         maximum-requests request-number ;
         quiet-period seconds ;
         (reauthentication seconds | no-reauthentication);
         retries number ;
         server-timeout seconds ;
         supplicant (multiple | single | single-secure);
         supplicant-timeout seconds ;
         transmit-period seconds ;
      }
      static mac-address {
         interface interface-name ;
         vlan-assignment address ;
      }
   }
   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>;
    }
}
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;
}
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 >
        <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 {
      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>;
}
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 ;
            }
            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 ;
        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  {
          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 ;
      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 {
                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>;
        }
    }
  }
}
```

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 Software.

Description Disable ES-IS globally or on an interface.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description Configure the ES-IS end system configuration timer.

Options *seconds*—How often a system reports its availability to other systems.
Default: 180 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

esis

Syntax esis { ... }

Hierarchy Level [edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable ES-IS.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

graceful-restart

Syntax
```
graceful-restart {
    disable;
    restart-duration seconds;
}
```

Hierarchy Level [edit protocols esis]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description Configure ES-IS on an interface.

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

all—Configure on all interfaces.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description Disable MAC learning for the entire device.

Default MAC learning is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description Configure Layer 2 address learning and forwarding properties globally.

The statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

Description Configure the ES-IS preference value.

Options *preference*—Preference value.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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.

Chapter 15

Routing-Instances Hierarchy

This chapter presents the complete routing-instances configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

Use the statements in the routing-instances configuration hierarchy to configure routing instances. For configuration instructions, see the *JUNOS Software Design and Implementation Guide*.

For information about these routing-instances statements that are shared across Juniper Networks devices, see the *JUNOS Routing Protocols Configuration Guide*, the *JUNOS Services Interfaces Configuration Guide*, the *JUNOS Multicast Protocols Configuration Guide*, and the *JUNOS Network Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Routing-Instances Configuration Statement Hierarchy on page 201

Routing-Instances Configuration Statement Hierarchy

To configure routing instances, use the following statements at the [edit routing-instances] hierarchy level.

Shared JUNOS statements in the routing-instances hierarchy are shown in normal font and are documented in the *JUNOS Routing Protocols Configuration Guide*, the *JUNOS Services Interfaces Configuration Guide*, the *JUNOS Multicast Protocols Configuration Guide*, and the *JUNOS Network Interfaces Configuration Guide*.

```
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;
        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 ;
            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>;
      }
   }
}
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
  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 ;
        }
    }
  }
}
```

Chapter 16

Routing-Options Hierarchy

This chapter presents the complete routing-options configuration hierarchy available on J series Services Routers and SRX Series Services Gateways running JUNOS Software.

Use the statements in the routing-options configuration hierarchy to configure protocol-independent routing properties. For configuration instructions, see the *JUNOS Software Design and Implementation Guide* and the *JUNOS Software Interfaces and Routing Configuration Guide*.

For information about these routing-options statements that are shared across Juniper Networks devices, see the *JUNOS Routing Protocols Configuration Guide*, the *JUNOS Services Interfaces Configuration Guide*, and the *JUNOS Multicast Protocols Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Routing-Options Configuration Statement Hierarchy on page 213

Routing-Options Configuration Statement Hierarchy

To configure routing options, use the following statements at the [edit routing-options] hierarchy level.

Shared JUNOS statements in the routing-options hierarchy are shown in normal font and are documented in the *JUNOS Routing Protocols Configuration Guide*, the *JUNOS Services Interfaces Configuration Guide*, and the *JUNOS Multicast Protocols Configuration Guide*.

```
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 {
      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 ;
      }
      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>;
      }
    }
```

Chapter 17

Schedulers Hierarchy and Statements

This chapter presents the complete schedulers configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. The chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the schedulers configuration hierarchy to determine the day and time when security policies are in effect. For configuration instructions, see the *JUNOS Software Security Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Schedulers Configuration Statement Hierarchy on page 221

Schedulers Configuration Statement Hierarchy

To configure security policy schedulers, use the following statements at the [edit schedulers] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

```
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);
        }
      }
    }
```

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 Software.

Description Schedule the security policy to be in effect for an entire day.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

schedulers

Syntax schedulers { ... }

Hierarchy Level [edit]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Chapter 18

Security Hierarchy and Statements

This chapter presents the complete **security** configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the **security** configuration hierarchy to configure the rules for the transit traffic and the actions that need to take place on the traffic as it passes through the firewall and to monitor the traffic attempting to cross from one security zone to another. For configuration instructions, see the *JUNOS Software Security Configuration Guide*.

For information about the following **security** statements that are shared across Juniper Networks devices—see the *JUNOS System Basics Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Security Configuration Statement Hierarchy on page 237
- no-allow-icmp-without-flow on page 524
- no-enable-all-qmodules on page 524
- no-enable-packet-pool on page 524
- no-log-errors on page 524
- no-policy-lookup-cache on page 525
- no-reset-on-policy on page 525

Security Configuration Statement Hierarchy

To configure security rules, actions, and zones, use the following statements at the **[edit security]** hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the **security** hierarchy are shown in normal font and are documented in the *JUNOS System Basics Configuration Guide* .

```
security {
    alg {
        dns {
            disable;
            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>;
                    }
                }
            }
        }
        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>;
      }
    }
}
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>;
        }
      }
    }
  authentication-key-chains {
    key-chain key-chain-name {
      description text ;
      tolerance seconds ;
    }
  }
  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) ;
      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;
        }
        iso {
            mode packet-based;
        }
        mpls {
            mode packet-based;
        }
    }
}
forwarding-process {
application-services {
        session capacity {
            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>;
          }
          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;
    }
}
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);
        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);
        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-notify>;
                    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;
            }
          }
          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;
    no–application—system—cache;
}
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;
    }
}
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;
        wildcard wildcard-string;
      }
      hostname domain-name;
      ike-user-type (group-ike-id | shared-ike-id);
      inet ip-address;
      user-at-hostname user-at-hostname;
    }
    external-interface external-interface-name;
    ike-policy policy-name;
    local-identity (distinguished-name string | hostname hostname
    | inet ipv4-ip-address | user-at-hostname e-mail-address);
    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>;
  }
  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);
        encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
        | aes-256-cbc);
    }
    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);
        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 ipv4-prefix;
               remote ipv4-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;
         }
      }
      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];
          source-address [source-address];
        }
        then {
          source-nat (off | interface | pool pool-name);
          persistent-nat {
            permit ( any-remote-host | target-host | target-host-port );
```

```
                inactivity-timeout seconds;
                max-session-number number;
            }
        }
    }
    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;
}
}
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;
    }
}
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 (wx-redirect | wx-reverse-redirect);
                    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-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;
            winnuke;
        }
        udp {
            flood {
                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 {
        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;
        }
        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];
       }
    }
}
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);
      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;
        }
    }
}
}
```

access profile

See the following sections:

- access-profile (Dynamic VPNs) on page 267
- access-profile (IPsec VPNs) on page 267

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 Software.

Description Specify the access profile to use for extended authentication for remote users trying to download the Access Manager.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 4294967295

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

action

Syntax

```
action {
   (close-client | close-client-and-server | close-server |
   drop-connection | drop-packet | ignore-connection |
   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 Software.

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.
- 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

action (AppDDoS)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

active-policy

Syntax active-policy *policy-name* ;

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

address

See the following sections:

- address (ARP Proxy) on page 274
- address (Destination NAT) on page 275
- address (IKE Gateway) on page 275
- address (Zone Address Book) on page 276
- address (Zone Address Set) on page 276

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

address (IKE Gateway)

Syntax address [(*ip-address* | *hostname*)];

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the IP address or the hostname of the primary Internet Key Exchange (IKE) gateway and up to four backup gateways.

Options *ip-address* | *hostname* —IP address or hostname of an IKE gateway.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

address (Zone Address Book)

Syntax address *address-name* *(ip-prefix* | dns-name *dns-address-name)* ;

Hierarchy Level [edit security zones security-zone *zone-name* address-book]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Add an entry containing an IP address or Domain Name System (DNS) hostname 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— IPv4 address with prefix.

dns-name *dns-address-name* —DNS address name.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

address (Zone Address Set)

Syntax address *address-name* ;

Hierarchy Level [edit security zones security-zone *zone-name* address-book address-set *address-set-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Add an address entry to a set of IP addresses for a security zone.

Options *address-name* —Address entry name, as defined with the address (Zone Address Book) statement.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

address-book

Syntax

```
address-book {
   address  address-name (ip-prefix |  dns-name  dns-address-name) ;
   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 Software.

Description Define entries in the address book of a security zone. An address book is a list containing all addresses and address groups, and domain names defined for a security zone. You use address-book entries to identify addressable entities in policy definitions.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter an address-blacklist (or whitelist) custom-object for local list spam filtering.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

address-persistent

Syntax address-persistent;

Hierarchy Level [edit security nat source]

Release Information Statement modified in Release 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter an address-whitelist (or blacklist) custom-object for local list spam filtering.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 100000 per second
Default: 512 per second

NOTE: For SRX Series devices the applicable range is 1 through 1000000 per second.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Set an alert flag in the Alert column of the Log Viewer for the matching log record.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

alg

Syntax

```
alg {
    dns {
        disable;
        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>;
            }
        }
    }
    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>;
      }
    }
  }
  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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

all-tcp

Syntax
```
all-tcp {
   mss  value ;
}
```

Hierarchy Level [edit security flow tcp-mss]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 65535 bytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

allow-dns-reply

Syntax allow-dns-reply;

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow an ICMP packet without matched request. By default the ICMP flow is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Instructs the device to send dead peer detection (DPD) requests regardless of whether there is outgoing IPsec traffic to the peer.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

antispam

See the following sections:

- antispam (feature-profile)
- antispam (utm-policy)

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 Software.

Description Configure UTM antispam features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

antivirus

See the following sections:

- antivirus (feature-profile)
- antivirus (utm-policy)

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 Software.

Description Configure UTM antivirus full and express features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow or deny access to specific Access Point Names (APNs)

- *pattern-string*—Sets an APN suffix such as “juniper.net.mcc123.mnc456.gprs”.
- **drop**—Specifies to deny GTP packets from all Selection Modes for this APN.
- **pass**—Specifies to permit GTP packets from all Selection Modes for this APN.
- **selection**—Specifies 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application

See the following sections:

- application (AppDDoS) on page 297
- application (Protocol Binding Custom Attack) on page 297
- application (Security Policies) on page 298

application (AppDDoS)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow IDP to match the attack for a specified application.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software 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;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application-screen

See the following sections:

- application-screen (H323) on page 299
- application-screen (MGCP) on page 300
- application-screen (SCCP) on page 300
- application-screen (SIP) on page 301

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 Software.

Description Configure the security screens for the H.323 protocol Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the security screens for the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the security screens for the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the security screens for the Session Initiation Protocol (SIP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application-services

See the following sections:

- application-services (priority) on page 302
- application-services (Unified Access Control) on page 303
- application-services (WXC Integrated Services Module) on page 303

application-services (priority)

Syntax

```
application-services {
maximize-idp-sessions {
   weight {
      equal;
         firewall;
      idp;
   }
   }
}
```

Hierarchy Level [edit security forwarding-process]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

Description You can configure the device to switch from an integrated firewall mode to maximize IDP mode to increase the capacity of IDP processing. 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.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 Enforcer in a UAC deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application-services (WXC Integrated Services Module)

Syntax application-services (wx-redirect | wx-reverse-redirect);

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 Software.

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 wx-redirect—Specify the WX redirection needed for the packets that arrive from the LAN.

wx-reverse-redirect—Specify the WX redirection needed for the reverse flow of the packets that arrive from the WAN.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

application-system-cache-timeout

Syntax application-system-cache-timeout *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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 1000000 seconds
Default: 3600 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 100000 per second
Default: 200 per second

NOTE: For SRX Series devices the applicable range is 1 through 1000000 per second.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

attacks

See the following sections:

- attacks (Exempt Rulebase) on page 306
- attacks (IPS Rulebase) on page 307

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

attack-type

See the following sections:

- attack-type (Anomaly) on page 308
- attack-type (Chain) on page 309
- attack-type (Signature) on page 310

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 Software.

Description Specify the type of attack.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 {
                    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 Software.

Description Specify the type of attack.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

authentication-algorithm

Syntax authentication-algorithm (md5 | sha1 | sha-256);

Hierarchy Level [edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

authentication-method

Syntax authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);

Hierarchy Level [edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Specifies 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—Specifies that the Digital Signature Algorithm (DSA) is used.

pre-shared-keys—Specifies 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—Specifies that a public key algorithm, which supports encryption and digital signatures, is used.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the automatic re-enrollment of a certificate authority (CA) certificate.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable the device to automatically download the updated signature database from the specified URL.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the tunnel interface to which the route-based virtual private network (VPN) is bound.

Options *interface-name* —Tunnel interface.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Apply protocol block command custom-objects to the content-filtering profile

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

c-timeout

Syntax c-timeout *minutes* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ca-identity

Syntax ca-identity *ca-identity* ;

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ca-profile

Syntax

```
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;
    }
}
```

Hierarchy Level [edit security pki]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Configure certificate authority (CA) profile.

Options *ca-profile-name* —Name of a trusted CA.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the name of the certificate authority (CA) profile.

Options *ca-profile-name* —Name of the specific CA profile.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

cache-size

Syntax cache-size *size*;

Hierarchy Level [edit security idp sensor-configuration log]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

Description Specify the size in bytes for each user's log cache.

Options size—Cache size.
Range: 1 through 65535 bytes
Default: 12800 bytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a category filter to add attack objects based on the category.

Options values—Name of the category filter.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Select a custom URL category list you created (custom objects) for filtering against.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

certificate

Syntax
```
certificate {
   local-certificate  certificate-id ;
   peer-certificate-type (pkcs7 | x509-signature);
   trusted-ca ( ca-index  | use-all);
}
```

Hierarchy Level [edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the certificate authority (CA) certificate to use for automatic re-enrollment.

Options *certificate-id-name* —Identifier of the certificate that needs automatic re-enrollment.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

container

Syntax container *container-string*;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic distinguished-name]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

content-filtering

See the following sections:

- content-filtering (feature-profile)
- content-filtering (utm-policy)

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 Software.

Description Configure UTM content-filtering features.

This statement is supported on J Series devices and SRX100, SRX210, SRX240, and SRX650 devices.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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]
```

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description If the content size exceeds a set limit, the content is either passed or blocked. The default action is BLOCK.

Options
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

context (AppDDoS)

Syntax context *context-name*;

Hierarchy Level [edit security idp application–ddos *name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

count

See the following sections:

- count (Custom Attack) on page 337
- count (Security Policies) on page 337

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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);
        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 {
                    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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter a custom message to be sent when HTTP requests are blocked.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

custom-message

See the following sections:

- custom-message (antivirus notification-options fallback-block/non-block)
- custom-message (antivirus notification-options virus-detection)
- custom-message (content-filter notification-options)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

custom-message (antivirus notification-options virus-detection)

Syntax custom-message *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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Custom message notifications are generally used when content is blocked by the content filter.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

custom-message-subject

See the following sections:

- custom-message-subject (antivirus notification-options fallback-block/non-block)
- custom-message-subject (antivirus notification-options virus-detection)
- custom-message-subject (antivirus pattern-update email-notify)

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure custom objects before configuring UTM feature-profile features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a custom string for identifying a message as spam.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the data path debugging options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

default

See the following sections:

- default (antivirus fallback-options)
- default (web-filtering fallback-settings)

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

default-policy

Syntax
```
default-policy {
   (deny-all | permit-all);
}
```

Hierarchy Level [edit security policies]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

deny

See the following sections:

- deny (Policy) on page 356
- deny (SIP) on page 357

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 Software.

Description Block the service at the firewall. The device drops the packets.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

description

See the following sections:

- description (IDP Policy) on page 358
- description (Security Policies) on page 358

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 Software.

Description Specify descriptive text for an exempt rule, or IPS rule.

Options *description* —Descriptive text about an exempt rule, or IPS rule.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

description (Security Policies)

Syntax description *description* ;

Hierarchy Level [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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

destination

See the following sections:

- destination (Destination NAT) on page 359
- destination (IP Headers in Signature Attack) on page 360

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

destination-address

See the following sections:

- destination-address (Destination NAT) on page 361
- destination-address (IDP Policy) on page 362
- destination-address (Security Policies) on page 362
- destination-address (Source NAT) on page 363
- destination-address (Static NAT) on page 363
- destination-address (Traffic Policy Services Gateway) on page 364

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software. Support for rulebase-ddos introduced in JUNOS 10.0.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a destination IP address or IP address set to be used as the match criteria for the security policy.

Options *address-name* —IP address, IP address set, or address book entry.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a destination address to match the rule. You can configure multiple addresses or subnets.

Options *destination-address* —Destination address or a subnet.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

destination-address (Traffic Policy Services Gateway)

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 Software.

Description Enable the destination address translation to permit the traffic. By default the policy permits both the translated and the untranslated packets.

Options drop-translated—Drop the packets with translated destination address.

drop-untranslated—Drop the packets without translated destination address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

destination-port

See the following sections:

- destination-port (Destination NAT) on page 367
- destination-port (Signature Attack) on page 367

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 Software.

Description Specify a destination port to match the rule. You can configure one port.

Options *port-number* —Destination port number.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 100000 per second
Default: 4000 per second

NOTE: For SRX Series devices the applicable range is 4 through 1000000 per second.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

detect-shellcode

Syntax detect-shellcode;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

Description Enable to detect the shell code and prevent buffer overflow attacks. By default this setting is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure protocol detector engine for a specific service.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

dh-group

Syntax dh-group (group1 | group2 | group5);

Hierarchy Level [edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

direction

See the following sections:

- direction (Custom Attack) on page 371
- direction (Dynamic Attack Group) on page 372

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Disable translation of the host IP address in call-ID header. Translation is enabled by default.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

distinguished-name

Syntax

```
distinguished-name {
    container   container-string  ;
    wildcard    wildcard-string  ;
}
```

Hierarchy Level [edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

dns

Syntax

```
dns {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

download-profile

See the following sections:

- download-profile (ftp antivirus utm-profile)
- download-profile (ftp content-filtering utm-profile)

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 Software.

Description Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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>;
```

```
}
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 Software.

Description Displays information about the configuration of the current GTP inspection.

- *number*—Specifies 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.

- **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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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;
user-at-hostname user-at-hostname;
```

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Specify the identifier for the remote gateway with a dynamic IP address. Use this statement to set up a VPN with a gateway that has an unspecified IP address.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

early-ageout

Syntax early-ageout *seconds* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 65535 seconds
Default: 20 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable all the qmodules of the global rulebase IDP security policy. By default all the qmodules are enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable the packet pool to use when the current pool is exhausted. By default packet pool is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

encryption-algorithm

Syntax encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);

Hierarchy Level [edit security ike proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

endpoint-registration-timeout

Syntax endpoint-registration-timeout *seconds* ;

Hierarchy Level [edit security alg h323]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

event-rate

Syntax Syntax event-rate *rate*

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Limits the rate (0 to 1500) at which logs will be streamed per second.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

exception

See the following sections:

- exception (antivirus mime-whitelist)
- exception (content-filter block-mime)

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 Software.

Description Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the content-filter to use an exception list to the MIME block list (custom objects).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a list of common context value patterns that should be excluded from AppDDoS detection. For example, if you have a Web server that receives a high number of HTTP requests on home/landing page, you can exclude it from AppDDoS detection.

Options *regular-expression* —List of patterns for exclusion. Example: **www.juniper.net** **www.acmegizmo.com**.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 mach, 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

external-interface

See the following sections:

- external-interface (IKE Gateway) on page 392
- external-interface (Manual Security Association) on page 392

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

fallback-options

See the following sections:

- fallback-options (antivirus juniper-express-engine)
- fallback-options (antivirus kaspersky-lab-engine)

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 Software.

Description Fallback options tell the system how to handle the errors.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

fallback-settings

See the following sections:

- fallback-settings (web-filtering surf-control-integrated)
- fallback-settings (web-filtering websense-redirect)
- fallback-settings (web-filtering juniper-local)

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 Software.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Fallback settings tell the system how to handle errors.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

family

Syntax

```
family {
    inet6 {
        mode packet-based;
    }
    iso {
        mode packet-based;
    }
    mpls {
        mode packet-based;
    }
}
```

Hierarchy Level [edit security forwarding-options]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Determine the protocol family to be used for packet forwarding.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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);
              }
              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 Software.

Description Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

filename-extension

Syntax
```
filename-extension {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description To create a dynamic attack group, set the criteria using the different type of filters.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable detection of an illegal combination of flags, and reject packets that have this combination.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

firewall-authentication

See the following sections:

- firewall-authentication (Policies) on page 406
- firewall-authentication (Security) on page 407

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 Software.

Description Configure firewall authentication methods.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

flood

See the following sections:

- flood (ICMP) on page 408
- flood (UDP) on page 409

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

flow

See the following sections:

- flow (IDP) on page 410
- flow (Security Flow) on page 411

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 Software.

Description Configure the IDP engine to manage the packet flow.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

- 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

force-upgrade

Syntax force-upgrade;

Hierarchy Level [edit security dynamic-vpn]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

forwarding-options

Syntax

```
forwarding-options {
    family {
        inet6 {
            mode packet-based;
        }
        iso {
            mode packet-based;
        }
    }
    mpls {
        mode packet-based;
    }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Determine how the inet6, and iso protocol families manage security forwarding options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

fragment

Syntax fragment;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

from-zone

See the following sections:

- from-zone (IDP Policy) on page 416
- from-zone (Security Policies) on page 417

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 Software. Support for rulebase-ddos introduced in JUNOS software 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 (wx-redirect | wx-reverse-redirect);
                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-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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ftp

Syntax

```
ftp {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of JUNOS Software.

Description Specify the FTP ALG on the device.

Options disable—Disable the FTP ALG. By default, the FTP ALG is enabled.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ftp (utm)

See the following sections:

- ftp (antivirus utm-policy)
- ftp (content-filtering utm-policy)

ftp (antivirus utm-policy)

Syntax
```
ftp {
upload-profile profile-name;
   download-profile profile-name;
}
```

Hierarchy Level [edit security utm utm-policy *policy-name* anti-virus]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Configure a UTM policy for the antivirus FTP protocol and attach this policy to a security profile to implement it.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a functional zone.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

gateway

See the following sections:

- gateway (IKE) on page 423
- gateway (IPsec) on page 424
- gateway (Manual Security Association) on page 424

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 ;
        user-at-hostname user-at-hostname ;
    }
    external-interface external-interface-name ;
    ike-policy name ;
    local-identity (hostname hostname | inet ipv4-ip-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 ike]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Configure an IKE gateway.

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

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

gateway (IPsec)

Syntax gateway *gateway-name* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the remote gateway.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description For a manual security association, specify the IP address of the peer. (This statement is not supported on dynamic VPN implementations.)

Options *ip-address* —IP address of the peer.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the global rulebase IDP security policy.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

gre-in

Syntax
```
gre-in {
   mss value ;
}
```

Hierarchy Level [edit security flow tcp-mss]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

gre-out

Syntax

```
gre-out {
    mss value ;
}
```

Hierarchy Level [edit security flow tcp-mss]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 65535 bytes
Default: 1320 bytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 {
            <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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure context hit rate thresholds to start bot client classifications for application-level 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 AppDDOS 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

high-watermark

Syntax high-watermark *percent* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Set server host parameters by entering the server name or IP address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

host (Security Logging)

Syntax host *ip-address*

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the base address of the original source IP address range. This is used for IP shifting.

Options *ip-address* —IPv4 address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Control the type of traffic that can reach the device from interfaces bound to the zone.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

hostname

Syntax hostname *domain-name* ;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Unique name by which a network-attached device is known on a network.

Options *domain-name* —A fully qualified domain name (FQDN).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

http-profile

See the following sections:

- http-profile (antivirus utm-policy)
- http-profile (content-filtering utm-policy)
- http-profile (web-filtering utm-policy)

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 Software.

Description Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the web-filtering HTTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

icmp

See the following sections:

- icmp (Protocol Binding Custom Attack) on page 439
- icmp (Security Screen) on page 440
- icmp (Signature Attack) on page 441

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 Software.

Description Allow IDP to match the attack for specified ICMP.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure ICMP intrusion detection service (IDS) options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow IDP to match the ICMP header information for the signature attack.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

identification

See the following sections:

- identification (ICMP Headers in Signature Attack) on page 442
- identification (IP Headers in Signature Attack) on page 443

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 ;
    }
    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];
```

```
        }
        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 ;
   }
   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 ;
        }
      }
      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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 {
                    alert;(
                }
            }
            severity (critical | info | major | minor | warning);
        }
    }
  }
}
```

Hierarchy Level [edit security idp]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

Description Configure a security IDP policy.

Options *policy-name* —Name of the IDP policy.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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;
        winnuke;
```

```
        }
        udp {
            flood {
                threshold  number ;
            }
        }
    }
}
```

Hierarchy Level [edit security screen]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Define screens for intrusion detection and prevention.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable the TCP reassembler to ignore the memory overflow to prevent the dropping of IDP custom applications. By default this feature is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable regular expression to detect intrusion attempts. By default this setting is disabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ike

See the following sections:

- ike (IPsec VPN) on page 456
- ike (Security) on page 457

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 ipv4-prefix ;
        remote ipv4-prefix ;
        service service-name ;
    }
}
```

Hierarchy Level [edit security ipsec vpn *vpn-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Define an IKE-keyed IPsec VPN.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 ;
            user-at-hostname  user-at-hostname ;
        }
        external-interface  external-interface-name ;
        ike-policy  policy-name ;
        local-identity (hostname  hostname  | inet  ipv4-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>;
    }
    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);
        encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
        | aes-256-cbc);
        lifetime-seconds  seconds ;
    }
    respond-bad-spi  number ;
    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 Software.

Description Define Internet Key Exchange (IKE) configuration.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ike-policy

Syntax ike-policy *policy-name* ;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the IKE policy to be used for the gateway.

Options *policy-name* —IKE policy name.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the type of IKE user for a remote access connection. (This statement is not supported on dynamic VPN implementations.)

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

imap-profile

See the following sections:

- imap-profile (antivirus utm-policy)
- imap-profile (content-filtering utm-policy)

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 Software.

Description Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

inactive-media-timeout

See the following sections:

- inactive-media-timeout (MGCP) on page 461
- inactive-media-timeout (SCCP) on page 461
- inactive-media-timeout (SIP) on page 462

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

inet

Syntax inet *ip-address* ;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify IPv4 address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

Options *ip-address* —IPv4 address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

inet6

Syntax
```
inet6 {
   mode packet-based;
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable the forwarding of IPv6 traffic. By default, the device drops IPv6 traffic.

NOTE: JUNOS Software security processing is not applied to IPv6 packets forwarded by the device.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

interface

See the following sections:

- interface (ARP Proxy) on page 465
- interface (Source NAT) on page 465

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

interface (Source NAT)

Syntax
```
interface {
   port-overloading { off };
}
```

Hierarchy Level [edit security nat source]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

Description Enable interface NAT with or without port overloading.

Options port-overloading—Specify off when persistent NAT is configured for interface NAT.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

interval

See the following sections:

- interval (IDP) on page 467
- interval (IKE) on page 467

interval (IDP)

Syntax interval *hours* ;

Hierarchy Level [edit security idp security-package automatic]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

interval (anti-virus)

See the following sections:

- interval (kaspersky-lab-engine)
- interval (juniper-express-engine)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

ip

See the following sections:

- ip (Protocol Binding Custom Attack) on page 469
- ip (Security Screen) on page 470
- ip (Signature Attack) on page 472

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.
- 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.
- 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.
- security-option—Detect packets where the IP option is 2 (security), and record the event in the SCREEN counters list for the ingress interface.
- 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.
- 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.
- 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.

- 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 tear-drop 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.
- unknown-protocol—Discard all received IP frames with protocol numbers greater than 137. Such protocol numbers are undefined or reserved.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

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 Software.

Description Allow IDP to match the IP header information for the signature attack.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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.

ip-action (AppDDoS)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Close future connections of any new sessions that match the IP action by sending RST packets to the client and server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Do not take any action against future traffic, but do log the event. This is the default.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure IPS security policy sensor settings.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the IPsec policy name.

Options *ipsec-policy-name* —Name of the IPsec policy.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ipsec-vpn

See the following sections:

- ipsec-vpn (Flow) on page 478
- ipsec-vpn (Policies) on page 478
- ipsec-vpn (Dynamic VPNs) on page 479

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 Software.

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 65535 bytes
Default: 1320 bytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define IPsec name for VPN.

Options *vpn-name* —Name of the IPsec.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Use this statement to specify which IPsec VPN configuration the dynamic VPN feature should use to secure traffic.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 1000000 microseconds
Default: 5000 microseconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

iso

Syntax
```
iso {
    mode packet-based;
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable the forwarding of IS-IS traffic. By default, the device drops IS-IS traffic.

NOTE: JUNOS Software security processing is not applied to IS-IS packets forwarded by the device.

Options The remaining statements are explained separately.

Usage Guidelines To configure the IS-IS protocol, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

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;
```

```
    }
}
```

Hierarchy Level [edit security utm feature-profile anti-virus]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Configure the UTM express antivirus feature.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the UTM web-filtering local feature.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Configure the UTM full file-based antivirus feature.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

land

Syntax land;

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

large

Syntax large;

Hierarchy Level [edit security screen ids-option *screen-name* icmp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Configure the device to detect and drop any ICMP frame with an IP length greater than 1024 bytes.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

lifetime-kilobytes

Syntax lifetime-kilobytes *kilobytes* ;

Hierarchy Level [edit security ipsec proposal *proposal-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

list

See the following sections:

- list (antivirus mime-whitelist)
- list (content-filter block-mime)

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 Software.

Description
Configure the antivirus scanner to use MIME bypass lists (custom objects).

Options
The remaining statements are explained separately.

Usage Guidelines
For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description
Configure the content filter to use MIME block lists (custom objects).

Options
The remaining statements are explained separately.

Usage Guidelines
For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

local

Syntax local *ipv4-prefix* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike proxy-identity]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Specify the local IP address and subnet mask for the proxy identity.

Options *ipv4-prefix* —IP address and subnet mask.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

local-certificate

Syntax local-certificate *certificate-id* ;

Hierarchy Level [edit security ike policy *policy-name* certificate]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

local-identity

Syntax local-identity (distinguished-name *string* | hostname *hostname* | inet *ipv4-ip-address* |
user-at-hostname *e-mail-address*);

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 IP 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 *ipv4-ip-address* —Specify identity as an IPv4 IP address.

user-at-hostname *e-mail-address* —Specify identity as an e-mail address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

log

See the following sections:

- log (GTP) on page 491
- log (IDP) on page 492
- log (IDP Policy) on page 492
- log (Security Policies) on page 493
- log (Security Logging) on page 494

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 Software.

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-limt (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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure IDP security policy logs.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Log the information about the IP action against the traffic that matches a rule.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable the log attacks to create a log record that appears in the log viewer.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the amount of time to supersede the IPS sensor logs.

Options *minimum-value* —Minimum time to supersede the log.
Range: 0 through 65535 seconds
Default: 1 second

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

low-watermark

Syntax low-watermark *percent* ;

Hierarchy Level [edit security flow aging]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define a manual IPsec security association (SA). (This statement is not supported on dynamic VPN implementations.)

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

match

See the following sections:

- match (Destination NAT) on page 499
- match (IDP Policy) on page 500
- match (rulebase-ddos) on page 501
- match (Security Policies) on page 501
- match (Source NAT) on page 502
- match (Static NAT) on page 502

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 Software.

Description Specify the destination rules to be used as match criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the rules to be used as match criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the rules to be used as match criteria for application-level DDoS protection.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure security policy match criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

match (Source NAT)

Syntax
```
match {
    destination-address [destination-address];
    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 Software.

Description Specify the source rules to be used as match criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the static rules to be used as match criteria.

Options The remaining statement is explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define the maximum TCP flow memory which IDP sensor can handle.

Options *value* —Maximum TCP flow memory in kilobytes.
Range: 64 through 4294967295 kilobytes
Default: 1024 kilobytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define the maximum TCP packet memory that the IDP sensor can handle.

Options *value* —Maximum TCP packet memory.
Range: 64 through 4294967295 kilobytes (KB)
Default: 262144 KB

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the maximum memory length of a packet in bytes.

Options *value* —Maximum memory length in bytes.
Range: 0 through 200000000 bytes
Default: 100000000 bytes

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

max-sessions

Syntax max-sessions *value* ;

Hierarchy Level [edit security idp sensor-configuration application-identification]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

maximize-idp-sessions

Syntax maximize-idp-sessions

Hierarchy Level [edit security forwarding-process application-services]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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*—Specifies an IMSI prefix.
- *string*—Specifies an APN.
- **drop**—Enables the security device to deny GTP packets from all Selection Modes for the specified APN.
- **selection**—Specifies 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

member

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 Software.

Description Create the list of member attacks.

Options *member-name* —Name of the member list.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

message-flood

See the following sections:

- message-flood (H323) on page 512
- message-flood (MGCP) on page 513

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 Software.

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 65535
Default: 1000

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

mime-pattern

Syntax
```
mime-pattern {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass various types of scanning.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the antivirus scanner to use MIME bypass lists and exception lists.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

mode

See the following sections:

- mode (Forwarding-Options) on page 517
- mode (Policy) on page 517
- mode (Security Logging) on page 518

mode (Forwarding-Options)

Syntax mode packet-based;

Hierarchy Level [edit security forwarding-options family]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Enable packet forwarding for the selected protocol family. By default, the device drops traffic for the protocol family.

Options packet-based— Perform simple packet forwarding.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

mode (Policy)

Syntax mode (aggressive | main);

Hierarchy Level [edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

mode (Security Logging)

Syntax mode (event | stream)

Hierarchy Level [edit security log]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

mpls

Syntax
```
mpls {
   mode packet-based;
}
```

Hierarchy Level [edit security forwarding-options family]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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

msrpc

Syntax

```
msrpc {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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];
            }
            then {
                source-nat (off | interface | pool  pool-name );
                persistent-nat {
                    permit ( any-remote-host | target-host | target-host-port );
                    inactivity-timeout seconds;
                    max-session-number number;
                }
            }
        }
        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 Software.

Description Configure Network Address Translation (NAT) for the SRX Series device.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

nat-keepalive

Syntax nat-keepalive *seconds* ;

Hierarchy Level [edit security ike gateway *gateway-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Select negate to exclude the specified pattern from being matched.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Disable the antireplay checking feature of IPsec. By default, antireplay checking is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

no-policy-lookup-cache

See policy-lookup-cache

no-reset-on-policy

See reset-on-policy

no-sequence-check

Syntax no-sequence-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

no-syn-check

Syntax no-syn-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

notification

Syntax

```
notification {
    log-attacks {
        alert;
    }
}
```

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

notification-options

See the following sections:

- notification-options (antivirus juniper-express-engine)
- notification-options (antivirus kaspersky-lab-engine)
- notification-options (content-filtering)

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 Software.

Description There are multiple notification options you can configure to trigger when a virus is detected.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description There are multiple notification options you can configure to trigger when a virus is detected.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description You can configure a message notification to trigger when a content filter is matched.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

notify-mail-sender

See the following sections:

- notify-mail-sender (antivirus fallback-block)
- notify-mail-sender (antivirus notification-options virus-detection)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

optimized

Syntax optimized;

Hierarchy Level [edit security ipsec vpn *vpn-name* vpn-monitor]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a source pool to use when the current address pool is exhausted.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

packet-filter

Syntax packet-filter;

Hierarchy Level [edit security datapath-debug]

Release Information Command introduced in Release 9.6 of JUNOS Software.

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 IPv4 address prefix.

protocol– Match IP protocol type.

source-port– Match TCP/UDP source port.

source-prefix– Source IPv4 address prefix.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 Web page 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

pattern-update

See the following sections:

- pattern-update (kaspersky-lab-engine)
- pattern-update (juniper-express-engine)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

peer-certificate-type

Syntax peer-certificate-type (pkcs7 | x509-signature);

Hierarchy Level [edit security ike policy *policy-name* certificate]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

perfect-forward-secrecy

Syntax perfect-forward-secrecy keys (group1 | group2 | group5);

Hierarchy Level [edit security ipsec policy *policy-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

permit

Syntax

```
permit {
    application-services (wx-redirect | wx-reverse-redirect);
    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-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 Software.

Description Specify the policy action to perform when packets match the defined criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Apply protocol permit command custom-objects to the content-filtering profile

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

persistent-nat

Syntax

```
persistent-nat {
    permit ( any-remote-host | target-host | target-host-port );
    inactivity-timeout seconds;
    max-session-number number;
}
```

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 Software.

Description Configure persistent NAT.

Options

any-remote-host—All requests from a specific internal IP address and port are mapped to the same external IP address and port. Any external host can send a packet to the internal host using the mapped external address.

target-host—All requests from a specific internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to an internal host only if the internal host had 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 external IP address and port. An external host can send a packet to an internal host only if the internal host had previously sent a packet to the external host's IP address and port.

inactivity-timeout—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. The default is 5 minutes. Enter a value from 60 through 7200.

max-session-number—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. The default is 30 sessions. Enter a value from 8 through 100.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure an IPsec profile to request digital certificates.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Related Topics *JUNOS Feature Guide* and the *JUNOS System Basics and Services Command Reference*

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 (wx-redirect | wx-reverse-redirect);
                    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-vpn vpn-name ;
                        pair-policy pair-policy ;
                    }
                }
                log {
                    session-close;
                    session-init;
                }
            }
        }
```

```
    }
    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 Software.

Description Configure network security policies.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

policy

See the following sections:

- policy (IKE) on page 550
- policy (IPsec) on page 551
- policy (Security) on page 552

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>;
}
```

Hierarchy Level [edit security ike]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Configure an IKE policy.

Options *policy-name* —Name of the IKE policy. The policy name can be up to 32alphanumeric characters long.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

policy (IPsec)

Syntax

```
policy policy-name {
    description description ;
    perfect-forward-secrecy keys (group1 | group2 | group5);
    proposal-set (basic | compatible | standard);
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Define an IPsec policy.

Options *policy-name* —Name of the IPsec policy.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 (wx-redirect | wx-reverse-redirect);
            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-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*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Define a security policy.

Options *policy-name* —Name of the security policy.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable cache to accelerate IDP policy lookup.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

policy-rematch

Syntax policy-rematch;

Hierarchy Level [edit security policies]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

pool

See the following sections:

- pool (Destination NAT) on page 554
- pool (Source NAT) on page 555

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 Software.

Description Define a destination NAT pool to identify the pool uniquely.

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

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define a source NAT pool to identify the pool uniquely.

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

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

pop3–profile

See the following sections:

- pop3-profile (antivirus utm-policy)
- pop3-profile (content-filtering utm-policy)

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 Software.

Description Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering POP3 protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

port-randomization

Syntax
```
port-randomization {
    disable;
}
```

Hierarchy Level [edit security nat source]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 1000000 microseconds
Default: 5000 microseconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

pptp

Syntax

```
pptp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable to pre-filter the shell code and protects it from buffer overflow attacks. By default this setting is enabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

pre-shared-key

Syntax pre-shared-key (ascii-text | hexadecimal);

Hierarchy Level [edit security ike policy *policy-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Define a preshared key for an IKE policy.

Options ascii-text—ASCII text key.

hexadecimal—Hexadecimal key.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Set the command to disable the server-to-client inspection.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

process-override

Syntax process-override;

Hierarchy Level [edit security idp sensor-configuration ips]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

Description Set the command to forcefully run the IDS inspection module even if there is no policy match.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

profile

See the following sections:

- profile (antispam sbl)
- profile (antivirus juniper-express-engine)
- profile (antivirus kaspersky-lab-engine)
- profile (content-filtering)
- profile (web-filtering surf-control-integrated)
- profile (web-filtering websense-redirect)
- profile (web-filtering juniper-local)

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 Software.

Description Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Create a profile for the Kaspersky Lab engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Create a profile for the Juniper express engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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>;
  }
```

```
    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 Software.

Description Create a profile for the gtp feature. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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);
    encryption-algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc
    | aes-256-cbc);
}
```

Hierarchy Level [edit security ike]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Define an IKE proposal.

Options *proposal-name* —Name of the IKE proposal. The proposal name can be up to 32alphanumeric characters long.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

proposal-set

See the following sections:

- proposal-set (IKE) on page 575
- proposal-set (IPsec) on page 576

proposal-set (IKE)

Syntax proposal-set <basic | compatible | standard>;

Hierarchy Level [edit security ike policy *policy-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify a set of default Internet Key Exchange (IKE) proposals. (This statement is not supported on dynamic VPN implementations.)

Options basic—Basic set of two IKE proposals:

- Proposal 1—Preshared key, Data Encryption Standard (DES) encryption, and Diffie-Hellman Group 1 and Secure Hash Algorithm 1 (SHA-1) authentication.
- Proposal 2—Preshared key, DES encryption, and Diffie-Hellman Group 1 and MD5 authentication.

compatible—Set of four commonly used IKE proposals:

- Proposal 1—Preshared key, triple DES (3DES) encryption, and G2 and SHA-1 authentication.
- Proposal 2—Preshared key, 3DES, and Diffie-Hellman Group 2 and MD5 authentication.
- Proposal 3—Preshared key, DES encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.
- Proposal 4—Preshared key, DES encryption, and Diffie-Hellman Group 2 and MD5 authentication.

standard—Standard set of two set of IKE proposals:

- Proposal 1— Preshared key, 3DES encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.
- Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define a set of default IPsec proposals. (This statement is not supported on dynamic VPN implementations.)

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 MD5 authentication.

compatible—Set of four commonly used IKE proposals:

- Proposal 1—Preshared key, triple DES (3DES) encryption, and G2 and SHA-1 authentication.
- Proposal 2—Preshared key, 3DES, and Diffie-Hellman Group 2 and MD5 authentication.
- Proposal 3—Preshared key, DES encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.
- Proposal 4—Preshared key, DES encryption, and Diffie-Hellman Group 2 and MD5 authentication.

standard—Standard set of two set of IKE proposals:

- Proposal 1— Preshared key, 3DES encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.
- Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and Diffie-Hellman Group 2 and SHA-1 authentication.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure options to protect servers against INVITE attacks.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

protocol

See the following sections:

- protocol (IPsec) on page 578
- protocol (Manual Security Association) on page 578
- protocol (IP Headers in Signature Attack) on page 579
- protocol (Signature Attack) on page 580

protocol (IPsec)

Syntax protocol (ah | esp);

Hierarchy Level [edit security ipsec proposal *proposal-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

Description Define the IPsec protocol for a manual or dynamic security association (SA).

Options ah—Authentication Header protocol.

esp—Encapsulating Security Payload (ESP) protocol.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 ;
    }
```

```
        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 Software.

Description Specify a protocol to match the header information for the signature attack.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description

Select a protocol that the attack uses to enter your network.

Options

The remaining statements are explained separately.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

protocol-command

Syntax
```
protocol-command {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

protocols

See the following sections:

- protocols (Interface Host-Inbound Traffic) on page 586
- protocols (Zone Host-Inbound Traffic) on page 588

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 Software.

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 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.
- vrrp—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

except—(Optional) except can only be used if all has been defined.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure Address Resolution Protocol (ARP) proxy.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

proxy-identity

Syntax
```
proxy-identity {
    local ipv4-prefix ;
    remote ipv4-prefix ;
    service service-name ;
}
```

Hierarchy Level [edit security ipsec vpn *vpn-name* ike]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

real

Syntax

```
real {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure TCP reassembler for IDP sensor settings.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the time before expiration as a percentage.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify recommended filter to add predefined attacks recommended by Juniper to the dynamic attack group.

Options values—Name of the recommended filter.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a Perl Compatible Regular Expression (PCRE) expression.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

reject-timeout

Syntax reject-timeout *value* ;

Hierarchy Level [edit security idp sensor-configuration flow]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

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 65535 milliseconds
Default: 300 milliseconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

remote

Syntax remote *ipv4-prefix* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* ike proxy-identity]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Specify the remote IP address and subnet mask for the proxy identity.

Options *ipv4-prefix* —IP address and subnet mask.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

remove-r6

Syntax **remove-r6**;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Enables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Select reset if the compound attack should be matched more than once within a single session or transaction.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

respond-bad-spi

Syntax respond-bad-spi *number* ;

Hierarchy Level [edit security ike]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

retain-hold-resource

Syntax retain-hold-resource;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the method the device uses to verify the revocation status of digital certificates.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

route-change-timeout

Syntax route-change-timeout *seconds* ;

Hierarchy Level [edit security flow]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

routing-instance

See the following sections:

- routing-instance (Destination NAT) on page 601
- routing-instance (Source NAT) on page 601

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

rsh

Syntax

```
rsh {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Ssoftware.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

rst-invalidate-session

Syntax rst-invalidate-session;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

rst-sequence-check

Syntax rst-sequence-check;

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

rtsp

Syntax

```
rtsp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

rule

See the following sections:

- rule (AppDDoS Rulebase) on page 606
- rule (Destination NAT) on page 607
- rule (Exempt Rulebase) on page 608
- rule (IPS Rulebase) on page 609
- rule (Source NAT) on page 610
- rule (Static NAT) on page 611

rule (AppDDoS 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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define a destination NAT rule.

Options *rule-name* —Name of the destination NAT rule.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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;(
            }
        }
        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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

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 {
            permit ( any-remote-host | target-host | target-host-port );
            inactivity-timeout seconds;
            max-session-number number;
        }
    }
}
```

Hierarchy Level [edit security nat source rule-set *rule-set-name*]

Release Information Statement modified in Release 9.6 of JUNOS Software.

Description Define a source NAT rule.

Options *rule-name* —Name of the source NAT rule.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define a static NAT rule.

Options *rule-name* —Name of the static NAT rule.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 seconds;
         }
      }
   }
}
```

Hierarchy Level [edit security idp idp-policy *policy-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the rulebase parameters for application-level DDoS attacks.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software 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

See the following sections:

- rule-set (Destination NAT) on page 613
- rule-set (Source NAT) on page 614
- rule-set (Static NAT) on page 615

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 Software.

Description Configure the set of rules for destination NAT.

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 Software 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 (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 {
                permit ( any-remote-host | target-host | target-host-port );
                inactivity-timeout seconds;
                max-session-number number;
            }
        }
    }
    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 Software.

Description Configure the set of rules for source NAT.

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 Software 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 (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 Software.

Description Configure the set of rules for static NAT.

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 Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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;(
            }
         }
         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 Software.

Description Configure the IPS rulebase to detect attacks based on stateful signature and protocol anomalies.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure UTM server-based antispam features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Enables server-based spam filtering
- no-sbl-default-server—Disables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

scan-options

See the following sections:

- scan-options (antivirus juniper-express-engine)
- scan-options (anti-virus kaspersky-lab-engine)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

scope

See the following sections:

- scope (Chain Attack) on page 624
- scope (Custom Attack) on page 625

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

screen

See the following sections:

- screen (Security) on page 627
- screen (Zones) on page 628

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;
            winnuke;
        }
```

```
        udp {
            flood {
                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 Software.

Description Configure security screen options.

Options *screen-name* —Name of the screen configured at security screen ids-options level.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify a security screen for a security zone.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

security-package

Syntax

```
security-package {
   automatic {
      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 Software.

Description Configure the device to automatically download the updated signature database from the specified URL.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

security-zone

Syntax

```
security-zone zone-name {
  address-book {
    address address-name (ip-prefix | dns-name dns-address-name);
    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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 ;
    }
    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 ;
        }
    }
    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 Software.

Description Configure various IDP parameters to match the properties of transiting network traffic.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enables or disables the GTP Sequence Number Validation feature.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Set server parameters by entering the server name or IP address.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

sessions

Syntax sessions *number* ;

Hierarchy Level [edit security idp sensor-configuration ssl-inspection]

Release Information Statement introduced in Release 9.3 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable traffic to which the policy applies to be logged at the end of a session.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable traffic to which the policy applies to be logged at the beginning of a session.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

sequence-number

See the following sections:

- sequence-number (ICMP Headers in Signature Attack) on page 636
- sequence-number (TCP Headers in Signature Attack) on page 637

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 4294967295

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

service

See the following sections:

- service (AppDDoS) on page 638
- service (Anomaly Attack) on page 638
- service (Dynamic Attack Group) on page 639
- service (Security IPsec) on page 639

service (AppDDoS)

Syntax service <dns | http>;

Hierarchy Level [edit security idp application-ddos *name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Service is the protocol whose anomaly is defined in the attack. IP, TCP, UDP, and ICMP are also valid as services.

Options *service-name*—Name of the protocol.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Related Topics system-services (Interface Host-Inbound Traffic)

system-services (Zone Host-Inbound Traffic)

severity

See the following sections:

- severity (Custom Attack) on page 640
- severity (Dynamic Attack Group) on page 641
- severity (IPS Rulebase) on page 642

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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);
        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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

smtp-profile

See the following sections:

- smtp-profile (antispam utm-policy)
- smtp-profile (antivirus utm-policy)
- smtp-profile (content-filtering utm-policy)

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 Software.

Description Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter the number of sockets used for communicating between the client and server. The default is 1.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

source

See the following sections:

- source (IP Headers in Signature Attack) on page 651
- source (Source NAT) on page 652

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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];
                source-address [source-address];
            }
            then {
                source-nat (off | interface | pool pool-name );
                persistent-nat {
                    permit ( any-remote-host | target-host | target-host-port );
                    inactivity-timeout seconds;
                    max-session-number number;
                }
            }
        }
        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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

source-address

See the following sections:

- source-address (Destination NAT) on page 654
- source-address (IDP Policy) on page 654
- source-address (Source NAT) on page 655
- source-address (Security Policies) on page 655

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 Software.

Description Specify source address to match the rule. You can configure multiple addresses or subnets.

Options *source-address* —Source address or a subnet.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software. 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify source address to match the rule. You can configure multiple addresses or subnets.

Options *source-address* —Source address or a subnet.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Define the matching criteria, which can include one or more IP addresses, address sets, or both in the from-zone zone.

Options *address-name* —IP addresses, address sets, or both are used for matching.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

source-nat

Syntax

```
source-nat (off | interface | pool pool-name);
  persistent-nat {
    permit ( any-remote-host | target-host | target-host-port );
    inactivity-timeout seconds;
    max-session-number number;
  }
```

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 Software.

Description Specify the action of the source NAT rule.

Options off — Do not perform the source NAT operation.

interface — Use egress interface IPv4 address to perform the source NAT.

pool — Use user-defined source NAT pool to perform the source NAT.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

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 Software.

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 100000 per second
Default: 4000 per second

NOTE: For SRX Series devices the applicable range is 4 through 1000000 per second.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

spi

Syntax spi *spi-value* ;

Hierarchy Level [edit security ipsec vpn *vpn-name* manual]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

sql

Syntax

```
sql {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

ssl-inspection

Syntax
```
ssl-inspection {
   sessions  number ;
}
```

Hierarchy Level [edit security idp sensor-configuration]

Release Information Statement introduced in Release 9.3 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure static NAT of SRX Series device.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

strict-syn-check

Syntax strict-syn-check

Hierarchy Level [edit security flow tcp-session]

Release Information Statement introduced in Release 9.4 of JUNOS Software.

Description Enables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

sunrpc

Syntax

```
sunrpc {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 9.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure the UTM web-filtering integrated feature.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable SYN-cookie defenses or SYN-proxy defenses against SYN attacks.

The 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

Related Topics attack-threshold

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 Software.

Description Enables 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

system-services

See the following sections:

- system-services (Interface Host-Inbound Traffic) on page 674
- system-services (Zone Host-Inbound Traffic) on page 676

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 Software.

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—Enables 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).
- xnm-ssl— Enable incoming JUNOScript-over-SSL traffic for all specified interfaces.
- xnm-clear-text—Enable incoming JUNOScript traffic for all specified interfaces.

except—(Optional) except can only be used if all has been defined.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Enables 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—Enables incoming traceroute traffic (UDP port 33434).

- xnm-ssl— Enable incoming JUNOScript-over-SSL traffic for all specified interfaces.
- xnm-clear-text—Enable incoming JUNOScript traffic for all specified interfaces.

except—(Optional) except can only be used if all has been defined.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

t1-interval

Syntax t1-interval *milliseconds* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

t4-interval

Syntax t4-interval *seconds* ;

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

talk

Syntax

```
talk {
   disable;
   traceoptions {
      flag {
         all <extensive>;
      }
   }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Matches traffic based on the source address, destination address, destination port, and protocol of the attack traffic. This is the default.
- 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

tcp

See the following sections:

- tcp (Protocol Binding Custom Attack) on page 681
- tcp (Security Screen) on page 682
- tcp (Signature Attack) on page 683

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 Software.

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 65535

maximum-port*port-number*—Maximum port in the port range.
Range: 0 through 65535

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

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

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;
    winnuke;
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Configure TCP-layer intrusion detection service (IDS) options.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 {
        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 Software.

Description Allow IDP to match the TCP header information for the signature attack.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enable the device to drop illegal TCP packets with a missing or malformed flag field.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

tcp-rst

Syntax tcp-rst;

Hierarchy Level [edit security zones security-zone *zone-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Set or unset a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify protocol anomaly condition to be checked.

Options *test-condition* —Name of the anomaly test condition.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

tftp

Syntax

```
tftp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Release 9.2 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

then

See the following sections:

- then (Destination NAT) on page 692
- then (IDP Policy) on page 693
- then (rulebase-ddos) on page 694
- then (Security Policies) on page 695
- then (Source NAT) on page 696
- then (Static NAT) on page 696

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 Software.

Description Specify the action to be performed when traffic matches the destination NAT rule criteria.

Options The remaining statement is explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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;
        }
    }
    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 Software.

Description Specify the action to be performed when traffic matches the defined criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the session action to be performed when traffic matches the defined criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

then (Security Policies)

Syntax

```
then {
    count {
        alarm {
            per-minute-threshold  number;
            per-second-threshold  number ;
        }
    }
    (deny | reject);
    permit {
        application-services (wx-redirect | wx-reverse-redirect);
        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-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 Software.

Description Specify the policy action to be performed when packets match the defined criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

then (Source NAT)

Syntax

```
then {
    source-nat (off | interface | pool  pool-name );
    persistent-nat {
        permit ( any-remote-host | target-host | target-host-port );
        inactivity-timeout seconds;
        max-session-number number;
    }
}
```

Hierarchy Level [edit security nat source rule-set *rule-set-name* rule *rule-name*]

Release Information Statement modified in Release 9.6 of JUNOS Software.

Description Specify the action to be performed when traffic matches the source NAT rule criteria.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Specify the action to be performed when traffic matches the static NAT rule criteria.

Options The remaining statement is explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow IDP to detect a sequence of the same attacks over a period of time.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 AppDDoS 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

timeout

See the following sections:

- timeout (GTP) on page 700
- timeout (IDP Policy) on page 700
- timeout (Security Screen) on page 701

timeout (GTP)

Syntax **timeout**;

Hierarchy Level [edit security gprs gtp profile *name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535 seconds
Default: 0 second

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

timeout (utm)

See the following sections:

- timeout (antivirus fallback-options)
- timeout (antivirus scan-options)
- timeout (antivirus trickling)
- timeout (web-filtering surf-control-integrated cache)
- timeout (web-filtering fallback-settings)
- timeout (web-filtering websense-redirect profile)

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

timeout (antivirus scan-options)

Syntax timeout *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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

timeout (antivirus trickling)

Syntax timeout *value*;

Hierarchy Level [edit security utm feature-profile anti-virus juniper-express-engine *profile-name* trickling]
[edit security utm feature-profile anti-virus kaspersky-lab-engine *profile-name* trickling]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

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. That is the Time-out Interval. By default, trickling is disabled.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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).

J Series devices and SRX100, SRX210, SRX240, and SRX650 devices.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 10 seconds.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software. Support for rulebase-ddos introduced in JUNOS release 10.0.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

too-many-requests

See the following sections:

- too-many-requests (antivirus fallback-options)
- too-many-requests (web-filtering fallback-settings)

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

traceoptions

See the following sections:

- traceoptions (firewall-authentication) on page 712
- traceoptions (H.323 ALG) on page 713
- traceoptions (Flow) on page 714
- traceoptions (firewall-authentication) on page 716
- traceoptions (IDP) on page 717
- traceoptions (IKE) on page 719
- traceoptions (IPsec) on page 720
- traceoptions (MGCP ALG) on page 721
- traceoptions (NAT) on page 722
- traceoptions (datapath-debug) on page 724
- traceoptions (PKI) on page 725
- traceoptions (Policies) on page 727
- traceoptions (SCCP ALG) on page 729
- traceoptions (Screen) on page 730
- traceoptions (Security) on page 732
- traceoptions (SIP ALG) on page 734

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 Software.

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 Software.

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.

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 Software.

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.

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 Software.

Description Enables 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 (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 Software.

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

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 Software.

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 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 Software.

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.

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 Software.

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 Software.

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.

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 processing 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 Software.

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..4294967295)

Usage Guidelines For configuration instructions and examples, see the JUNOS Software Security Configuration Guide.

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

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 Software.

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.

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 Software.

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.

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 Software.

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.

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 Software.

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

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.

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 Software.

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.

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 Software.

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.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

transaction-timeout

Syntax transaction-timeout *seconds* ;

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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*]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Trickling applies only to HTTP. HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

trusted-ca

Syntax trusted-ca (*ca-index* | use-all);

Hierarchy Level [edit security ike policy *policy-name* certificate]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

tunnel

Syntax
```
tunnel {
    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 Software.

Description Encapsulate outgoing IP packets and decapsulate incoming IP packets.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

type

See the following sections:

- type (ICMP Headers in Signature Attack) on page 739
- type (Dynamic Attack Group) on page 739

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

type (utm)

See the following sections:

- type (antivirus fallback-block)
- type (antivirus notification-options virus-detection)
- type (content-filtering notification-options)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

udp

See the following sections:

- udp (Protocol Binding Custom Attack) on page 742
- udp (Security Screen) on page 743
- udp (Signature Attack) on page 744

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 Software.

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 65535

maximum-port*port-number*—Maximum port in the port range.
Range: 0 through 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

udp (Security Screen)

Syntax

```
udp {
    flood {
        threshold  number ;
    }
}
```

Hierarchy Level [edit security screen ids-option *screen-name*]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Allow IDP to match the UDP header information for the signature attack.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

unknown-message

See the following sections:

- unknown-message (H.323 ALG) on page 745
- unknown-message (MGCP ALG) on page 746
- unknown-message (SCCP ALG) on page 747
- unknown-message (SIP ALG) on page 748

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 Software.

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—Specifies that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Specifies that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Specifies that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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—Specifies that unknown messages be allowed to pass if the session is in NAT mode.

permit-routed— Specifies that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

upload-profile

- upload-profile (ftp antivirus utm-profile)
- upload-profile (ftp content-filtering utm-profile)

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 Software.

Description Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

url

Syntax url *url-name* ;

Hierarchy Level [edit security idp security-package]

Release Information Statement introduced in Release 9.2 of JUNOS Software.

Description Specify the URL to automatically download the updated signature database.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

url (antivirus)

See the following sections:

- url (kaspersky-lab-engine)
- url (juniper-express-engine)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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 Software.

Description This is a global blacklist category, blocking content for web-filtering.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

url-pattern

Syntax
```
url-pattern {
value [list];
}
```

Hierarchy Level [edit security utm custom-objects]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Use URL Pattern Lists to create Custom URL Category Lists. These are lists of patterns that bypass scanning.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

url-whitelist

See the following sections:

- url-whitelist (antivirus)
- url-whitelist (web-filtering)

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

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

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

user

Syntax
```
user {
    username;
}
```

Hierarchy Level [edit security dynamic-vpn client *configuration-name*]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Use this statement to specify which users can access the selected dynamic VPN configuration.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

user-at-hostname

Syntax user-at-hostname *user-at-hostname* ;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Configure an e-mail address. (This statement is not supported on dynamic VPN implementations.)

Options *user-at-hostname* —Valid e-mail address.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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;
   }
```

```
    }
}
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]

Release Information Statement introduced in Release 9.5 of JUNOS Software.

Description Configure UTM features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Ssoftware.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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 AppDDoS 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

Description Configure a notification to send when a virus is detected.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 ipv4-prefix ;
        remote ipv4-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 Software.

Description Configure an IPsec VPN.

Options *vpn-name* —Name of the VPN.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Topics dead-peer-detection

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

Description Optionally, redirect HTTP requests to the device's internal Web server by sending a redirect HTTP response to the client system to reconnect to the Web server 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

wildcard

Syntax wildcard *string*;

Hierarchy Level [edit security ike gateway *gateway-name* dynamic distinguished-name]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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 65535

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

winnuke

Syntax
```
winnuke;
```

Hierarchy Level [edit security screen ids-option *screen-name* tcp]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

Description Specifies 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Topics profile statement in the *JUNOS Systems Basics 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 );
            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]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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 like 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Chapter 19

Services Hierarchy and Statements

This chapter presents the services configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

For information about services statements that are shared across Juniper Networks devices, see the *JUNOS Services Interfaces Configuration Guide*.

For additional information about services statements that pertain to Integrated Convergence Services, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

NOTE: For the current release, the configuration hierarchy does not show the Integrated Convergence Services statements. However, the statements are included in the chapter.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- Services Configuration Statement Hierarchy on page 773

Services Configuration Statement Hierarchy

To configure RPM probes, use the following statements at the [edit services] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS Software statements in the services hierarchy are shown in normal font and are documented in the *JUNOS Services Interfaces Configuration Guide*.

```
services {
    rpm {
        bgp {
            data-fill;
            data-size;
            destination-port;
```

```
            history-size;
            logical-system logical-system-name [routing-instances routing-instance-name
              ];
            probe-count count ;
            probe-interval seconds ;
            probe-type type ;
            routing-instances instance-name ;
            test-interval interval ;
          }
          probe owner {
            test test-name {
              data-fill data ;
              data-size size ;
              destination-interface interface-name ;
              destination-port port ;
              dscp-code-point dscp-bits ;
              hardware-timestamp;
              history-size size ;
              probe-count count ;
              probe-interval seconds ;
              probe-type type ;
              routing-instance instance-name ;
              source-address address ;
              target-url ( url | address );
              test-interval interval ;
              thresholds thresholds ;
              traps traps ;
            }
          }
          probe-limit;
          probe-server {
            icmp {
              destination-interface interface-name ;
            }
            tcp {
              destination-interface interface-name ;
              port port-number ;
            }
            udp {
              destination-interface interface-name ;
              port port-number ;
            }
          }
        }
      }
```

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics infranet-controller

address (peer call server)

Syntax address (fqdn *fqdn* | ipv4–addr *ipv4–address*);

Hierarchy Level [edit services real-time-media peer-call-server address]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

Description Specify the address of the peer call server to be used by the media gateway. The media gateway directs certain calls to the peer call server for call handling and routing. The survivable call service monitors the health of the peer call server to determine if it is still able to provide those services.

Options *address*—The address of the peer call server, expressed in one of the following formats:

- *fqdn*—fully qualified domain name (FQDN)
- *ipv4-addr*—IPv4 address
- *ipv6-addr*—IPv6 address

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

analog (station-type)

Syntax

```
analog {
    template analog-template-name;
    tdm-interface interface;
    time-slot timeslot-number;
}
```

Hierarchy Level [edit services convergence-services station *station-name* station-type]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description For an analog station, specify the station type as analog. In addition to standard station configuration parameters, specify the interface for the station and, optionally, an analog template to be used. For a T1 CAS interface, specify the timeslot to be used.

The analog station inherits characteristics defined by an analog template assigned to it, including whether caller ID information is transmitted to destination parties and whether voice activity detection (VAD) and comfort noise generation are used. These parameters are enabled by default. You can use an analog template to disable them.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

analog-template

Syntax

```
analog-template analog-template-name; {
    caller-id-transmit;
    voice-activity-detection;
    comfort-noise-generation;
    class-of-restriction class-of-restriction-configuration;
}
```

Hierarchy Level [edit services convergence-services station-template]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Define an analog template to be applied to one or more analog stations. Parameters associated with the template are inherited by the station. For example, if caller ID transmit which is enabled by default, is disabled in the template, the feature is disabled for all stations that the template is assigned to.

You can configure multiple analog templates. For example, you might create one template for analog POTS (Plain Old Telephone System) telephones and call it pots-phone-template.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

auth-id (peer-call-server)

Syntax auth-id *authentication-id*

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the authentication ID to be used by the media gateway to authenticate to the peer call server.

- The authentication information for the media gateway is configured at the peer call server and the authentication ID (and password) credentials that you configure must match them.
- An authentication ID is required only if the peer call server challenges the media gateway to authenticate when it registers with it.

Administrators at the media gateway site and the peer call server site must communicate to coordinate this information.

Options *authentication-id*—The authentication ID to be used by the media gateway to authenticate to the peer call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

auth-id (station)

Syntax auth-id *authentication-id*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the authentication ID for the station to authenticate either to the peer call server (analog stations) or to the SRX SCS (SIP stations).

The authentication ID is used by stations in the following ways:

- For analog stations. When the peer call server is in control, local analog stations must authenticate to it, if the peer call server requires them to do so. Analog stations communicate with the peer call server via the media gateway.

  When the SRX SCS is in control, analog stations do not need to authenticate to it because they are physically connected to the device. By default, the user's station extension number is used.

- For SIP stations. When the SRX SCS is in control, local SIP stations authenticate to it. Previously they were registered with the peer call server. Because they are not directly connected to the SRX210 or the SRX240 device, they must register to the SRX SCS.

Options *authentication-id*—The authentication ID to be used for the station.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

auth-password (peer-call-server)

Syntax auth-password *authentication-password*;

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the authentication password to be used by the media gateway to authenticate to the peer call server.

- The authentication information for the media gateway is configured at the peer call server.
- The authentication password (and ID) credentials that you configure must match those configured at the peer call server.
- An authentication password is required only if the peer call server challenges the media gateway to authenticate when it registers with it. The password that you configure is secret; It is not displayed.

Administrators at the media gateway site and the peer call server site must communicate to coordinate this information.

Options *authentication-password*—The authentication password to be used by the media gateway to authenticate itself to the peer call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

auth-password (station)

Syntax auth-password *authentication-password*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the authentication password for the station to authenticate to the peer call server.

When the peer call server is in control, local analog stations must authenticate to it, if the peer call server requires them to do so. Analog stations communicate with the peer call server via the media gateway.

The password that you configure is secret, and not displayed.

Options *authentication-password*—The authentication password to be used by the media gateway to authenticate itself to the peer call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

auto-attendant

Syntax

```
auto-attendant {
   live-attendant {
      extension extension-number;
      hours {
         start-time start-time;
         end-time end-time;
      }
      ring-count number-of-rings;
   }
}
```

Hierarchy Level [edit services convergence-services features]

Description Enables auto-attendant when the operator, referred to as a live attendant, is unavailable to take calls and direct them to their intended parties. Specify the number of times the live attendant's phone should ring before the call is passed to auto-attendant.

Calls are forwarded to auto-attendant when the live attendant is busy, away from the phone, or after business hours. When a call is forwarded to auto-attendant, the following message is played:

"Welcome to the Unified Convergence Services automated attendant. Please enter your party's extension or press 1 to reach voicemail."The user can enter the destination party's extension number and be directed to it by auto-attendant.

If a user knows the external telephone number (DID) of a person at the branch and dials that number, auto-attendant is bypassed. By default, auto-attendant is enabled.

Options The remaining statements are described separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics server-certificate-subject

caller-id-transmit (analog template, sip-template)

Syntax caller-id-transmit statement

Hierarchy Level [edit services convergence-services station-template analog-template *analog-template-name*]
[edit services convergence-services station-template sip-template *sip-template-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Disable or enable use of the caller ID transmit feature for SIP templates and analog templates. Stations that the template is applied to inherit the state.

Use caller ID transmit as a toggle. Here is how it works:

- By default, caller ID transmit is enabled. You do not need to specify it in a template if you want it enabled.
- To disable the feature, specify caller-id-transmit disable in a template. To enable it after it has been disabled, specify caller-id-transmit in the template.
- For station configurations without SIP templates, caller ID transmit is enabled.
- Caller ID transmit works with the station's caller ID parameter. When caller ID transmit is enabled, user information configured for the caller-id parameter, such as the telephone number and the user's name, is sent to all destination (called) parties. If no user information is configured, the station's extension is transmitted.
- Normally the user's caller ID information is sent between the first and second telephone rings.

Options The remaining statements are described separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

call-type (policy)

Syntax call-type *class-of-call*;

Hierarchy Level [edit services convergence-services class-of-restriction *class-of-restriction-configuration* policy *policy-name* permission (allow | deny)]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the call-type parameter to indicate the kind of call that the policy which includes the parameter applies to. The policy specifies whether the call is allowed or denied.

You define policies for class-of-restriction configurations. You can define policies for inter-branch, local, long-distance, and international types of calls.

A class-of-restriction configuration is applied to a station or a station templateCalss. If a policy specifies that a type of call is allowed and its configuration is applied to a station, a user can make the call from the station's telephone and the call will be routed. A class-of-restriction configuration assigned to a station takes precedence when it also includes a template that specifies a class-of-restriction configuration.

You can configure many policies for a single class-of-restriction configuration, but you must configure each one separately.

By default, all classes of calls are denied except emergency calls and intra-branch calls. You must explicitly specify a policy in a class-of-restriction configuration to specify that a type of call is allowed. The called number must match a digit pattern in the SRX SCS dial plan for the call to be routed.

NOTE: The trunk-call type of call is an exception. The media gateway dial plan can include route patterns for the trunk-call call type, but no class-of-restriction is required for them.

The call-type statement for class-of-restriction policies is applicable when the SRX SCS is in control.

Options *class-of-call*—Type of call for which a policy is defined.

- inter-branch-call—Specifies whether calls to other branches are allowed.
- intra-branch-call—Calls made by users from one telephone to another within the branch. They are allowed by default. You cannot change the permission to deny intra-branch calls. Do not specify intra-branch-call as part of a class-of-restriction configuration. It is mentioned here for completeness.
- international-call—Specifies whether international calls are allowed.

  International calls are calls made to other countries. They are placed using an access code followed by an ITU-assigned country code and full subscriber number, including area code or city codes.

- local-call—Specifies whether local calls are allowed.

  Local calls are calls within the same geographic area. They are usually free but might incur per-minute or per-call charges.

- long-distance-call—Specifies whether long-distance calls are allowed.

  Long-distance calls, also referred to as toll calls, are directed to numbers outside the local area. They commonly require an access code and area code in addition to the subscriber number. Although less common today, in the past they also incurred a per-minute toll.

- *custom-call*—Specifies whether a user-defined custom call type is allowed.

  Custom calls are types of calls other than the predefined call types which you define. You can create multiple custom calls. For example, you might want to create a custom call called “westford-to-bangalore-allow” to allow inter-branch calls made from Westford to Bangalore exclusively.

- emergency-call—Emergency calls can be made by all users at the local branch, including users of SIP phones that are not configured.

  You cannot change the permission to deny the emergency call type. Do not specify the emergency-call call type as part of a class-of-restriction configuration. It is mentioned here for completeness.

  Emergency call digit patterns differ across countries. The SRX SCS routes all emergency calls to its local PSTN.

- any-*-call—Specifies that any type of call is allowed.

Only one type of call applies to the media gateway, the trunk call.

trunk-call—Used by the peer call server to route calls back through the media gateway trunks to the PSTN.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

call-type (route pattern)

Syntax call-type *class-of-call*;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-pattern *digit-pattern*]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

Description Specify a type of call for a route pattern entry in the dial plan.

Digit patterns might be patterns that many numbers could match. They can also be fully expressed numbers:

- For example, a digit pattern might specify the pattern for calls to extensions at another branch. Individual calls that match the pattern are routed to the branch. A server at the branch might forward the calls to individuals.
- A dial plan can contain multiple route patterns for the same type of call. For example, for the international call type, you might define several route patterns for digit patterns with different county codes.
- Digit patterns might also be fully-expressed numbers, such are direct-inward-dialing numbers. For example, a digit pattern might specify the complete number for a fax machine at the branch.

  Given availability of configured trunks, calls for fully-expressed numbers are routed more quickly than called numbers that match digit patterns because the MGW SCS does not need to resolve them.

If the call that the user places is permitted for the station based on its class-of-restriction policies, then the call is routed to its destination party using one of the trunks specified for the route pattern. Otherwise, the call is denied, in which case the following message is played to the user:

"The number you are dialing cannot be called from this station."

All types of calls except trunk calls apply to the SRX SCS only. The trunk call type of call applies to the media gateway only.

Options *class-of-call*—Type of call to be routed if its digit pattern matches the digit pattern of a route pattern in the dial plan and the call type is permitted for the station from which the call was made.

- interbranch-call—Specifies whether calls to other branches are allowed.
- intrabranch call—These calls are made by users from one telephone to another within the branch.

  They are allowed by default. You cannot change the permission to deny intrabranch calls. Do not specify intrabranch-call as part of a class-of-restriction configuration. It is mentioned here for completeness.
- international-call—Specifies whether international calls are allowed.

International calls are calls made to other countries. They are placed using an access code followed by an ITU-assigned country code and full subscriber number, including area code or city codes.

- local-call—Specifies whether local calls are allowed.

  Local calls are calls within the same geographic area. They are usually free but might incur per-minute or per-call charges.

- long-distance-call—Specifies whether long-distance calls are allowed.

  Long-distance calls, also referred to as toll calls, are directed to numbers outside the local area. They commonly require an access-code and area code in addition to the subscriber number. Although less common today, in the past they also incurred a per-minute toll.

- custom call—Specifies whether a user-defined custom call is allowed.

  Custom calls are types of calls other than the predefined call types. You can create multiple custom calls. For example, you might create a custom call called "westford-to-bangalore-allow" to allow interbranch calls made from Westford to Bangalore exclusively.

- emergency-call—Emergency calls can be made by all users at the local branch, including users of SIP phones that are not configured.

  You cannot change the permission to deny the emergency call type. Do not specify the emergency-call call type as part of a class-of-restriction configuration. It is mentioned here for completeness.

  Emergency call digit patterns differ across countries. The SRX SCS routes all emergency calls to its local PSTN.

- any--call—Specifies that any type of call is allowed.
- trunk-call—Used by the peer call server to route calls back through the media gateway trunks out to the PSTN.

NOTE: Only one type of call applies to the media gateway, the trunk call.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

cas-group

Syntax

```
cas-group {
time-slots time-slots;
signaling {
   fxo-loop-start;
   fxo-ground-start;
   fxs-loop-start;
   fxs-ground-start;
   em-wink-start;
}
}
```

Hierarchy Level [edit services convergence-services trunk *trunk-name* trunk-type t1

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure channel associated signaling (CAS) for T1 interfaces. CAS specifies a signaling method in which the signal is associated with the channel. Each of the time slots for the preconfigured T1 interface is associated with an individual channel. The 24 channels together form a frame. A T1 interface can carry up to 24 calls using two-wire pairs.

Specify the range of time slots or individual time slots dedicated to voice on the preconfigured interface. The system keeps track of which time slots are in use and sends a call out on the next available channel. For T1 interfaces, CAS uses a technique referred to as robbed bit signaling, in which an additional bit taken from the T1 frame is used for framing synchronization.

Options *time-slots*: Range of time slots on the T1 interface to be use for voice. Specify the time slots to be used in the following format, for example 1-5, 9.

signaling:

- Loop start—Signaling for FXO interfaces or FXS interfaces (fxo-loop-start or fxs-loop-start). Loop start signaling is one of the simplest forms of CAS signaling. When the handset is picked up (the telephone goes off-hook), it closes the circuit that draws current from the telephone company (telco) and indicates a change in status, which signals the telco company to provide a dial tone. An incoming call is signaled from the telco to the handset by sending a signal in a standard on/off pattern, which causes the telephone to ring.
- Ground start—Signaling for FXO interfaces or FXS interfaces (fxo-ground-start or fxs-ground-start). Ground-start signaling is a technique in which a party gets a dial tone by momentarily grounding one side of a two-wire trunk.
- em-wink-start—Ear-and-mouth-wink start is an in-band signaling method that defines a trunk-circuit side and a signaling unit side for each connection.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

class-of-restriction

Syntax

```
class-of-restriction class-of-restriction-configuration; {
    policy policy-name; {
        permission (allow | deny);
    call-type class-of-call;
    }
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Define a class-of-restriction configuration whose policy specifies a type of call and whether a user is allowed to place that kind of call from the station that the configuration is assigned. The SRX Series survivable call server (SRX Series SCS) uses class-of-restriction configurations in conjunction with its dial plan to determine whether a call can be routed.

You can create multiple class-of-restriction policies to allow or deny permission to make different types of calls, such as long-distance and international, but each policy must be configured separately. You cannot create one class-of-restriction configuration composed of multiple policies.

NOTE: Class-of-restriction policies do not apply to the trunk-call call type. The trunk call type of call applies to the media gateway dial plan only.

For each policy, specify the type of call and whether it is allowed or denied. Call types include emergency, intra-branch, inter-branch, local, long-distance, international, and custom calls. Intra-branch and emergency call types are not configurable within class of restriction policies. They are allowed by default.

NOTE: By default all calls except emergency and intra-branch calls are denied. For all other calls, you must create policies that allow them. (You can also explicitly specify that a type of call is denied).

Class of restriction configurations are applied to stations. Policies determine the types of calls a user can make. For example, a policy might give a user permission to make long-distance calls. Another policy assigned to the same class-of-restriction configuration might but deny them the ability to make international calls. The called number must also match a route pattern entry in the dial plan for it to be routed.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

class-of-restriction (station)

Syntax class-of-restriction *class-of-restriction-configuration*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a predefined class of restriction configuration containing one or more policies each of which specifies a type of call and whether the call is allowed or denied.

When you apply a class of restriction configuration to a station, its policies are enforced for that station. For example, if a policy specifies that international calls are allowed and the configuration containing that policy is applied to a station, the user of that station's telephone is permitted to make an international call, given that the SRX SCS dial plan supports it. .

Apart from the trunk call type which applies to the media gateway only, class of restriction policies are effective when the SRX SCS is in control.

NOTE: Emergency and intra-branch calls are allowed by default for all stations.

Options *class-of-restriction-configuration*—Name of a predefined configuration.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

class-of-restriction (analog template, sip template)

Syntax class-of-restriction *class-of-restriction-configuration*;

Hierarchy Level [edit services convergence-services station-template analog-template *analog-template-name*]
[edit services convergence-services station-template sip-template *sip-template-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description For the analog template or the sip template, specify the name of a predefined class of restriction configuration containing one or more policies each of which specifies a type of call and whether the call is allowed or denied.

When you apply a template to a station, its parameter values are assigned to the station. If the station does not have a class of restriction configuration, the one specified by the template applies to it, and its policies are enforced for the station. For example, if a policy specifies that international calls are allowed, the station's telephone user is permitted to make an international call.

NOTE: If both the station and the template specify a class-of-restriction configuration, the station's configuration takes precedence over the template's.

Apart from the trunk call type which applies to the media gateway only, class of restriction policies are effective when the SRX SCS is in control.

NOTE: Emergency and intra-branch calls are allowed by default for all stations.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

codec (peer call server)

Syntax codec [*preferred-codecs*];

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify one or more of the supported codecs in the order of precedence in which they should be used and negotiated with the peer call server until a common one is found. If the peer call server does not support the suggested codecs, it responds with a list of the codecs that it supports.

Options *preferred-codecs*—One or more codecs, specified in order of precedence. The following codecs are supported:

- G711-A—A13-bit PCM 8-kHz sample, 64 Kbps bitstream
- G711-μu—14-bit PCM 8-kHz sample, 64 Kbps bitstream
- G729AB—CS-ACELP, 8 Kbps bitstream

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

codec (sip template)

Syntax codec [*preferred-codecs*];

Hierarchy Level [edit services convergence-services station-template sip-template]]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify one or more of the supported codecs for the station in order of precedence to be used for the SIP station. The codecs are negotiated until a common one is found.

Options *preferred-codecs*—One or more codecs, specified in order of precedence. The following codecs are supported:

- G711-A—A13-bit PCM 8-kHz sample, 64 kbps bitstream
- G711-μu—14—bit PCM 8-kHz sample, 64 kbps bitstream
- G729AB—CS-ACELP, 8 kbps bitstream

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

description (peer call server)

Syntax description *server-description*;

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Provide a description of the peer call server to identify it. The description information, such as the server location, can help to identify the server, as a reminder..

Options *server-description*—Descriptive information about the peer call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

description (trunk groups)

Syntax description *trunk-group-description*;

Hierarchy Level [edit services convergence-services trunk-group]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Provide a description for the trunk group you are configuring. Trunk groups are used in a route pattern of a dial plan for either the media gateway (SRX Series MGW) or the SRX SCS (SRX Series SCS). A trunk group is composed of one or more trunks. A description might identify the type of trunks included in the group. Trunks contained in trunk groups are used to route calls from the branch to the PSTN.

Options *trunk-group-description*—Information about the trunk group.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

dial-plan (media gateway)

Syntax dial-plan *dial-plan-name*;

Hierarchy Level [edit services convergence-services media-gateway *media-gateway-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a preconfigured media gateway dial plan that includes one or more route patterns identifying a digit-pattern against which called numbers are matched and the trunks to be used to route matching calls out the media gateway trunks.

When the peer call server receives an outgoing call from the media gateway, it processes it and then routes it appropriately. It routes some outgoing calls to the branch's local PSTN through media gateway trunks and some through its own trunks to its local PSTN, depending on which circumstance is more appropriate and least costly.

The peer call server administrator tells the media gateway administrator the digit patterns to use for route patterns configured in the media gateway dial plan. To determine the trunks to be used for calls matching various digit patterns, the media gateway administrator can provision trunks by creating trunk groups and then assigning them to specific route patterns.

For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

dial-plan (survivable call server)

Syntax dial-plan *dial-plan-name*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a preconfigured dial plan to be used for the survivable call server. The survivable call server dial plan can include all call types that are predefined and custom call types except the trunk-call call type.

The survivable call server dial plan should emulate the peer call server dial plan. The survivable call server assumes responsibility for the peer call server, and it should route the calls similarly unless other circumstances require differently.

Options *dial-plan-name*—Name of a preconfigured dial plan to be used for the survivable call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

digit-manipulation

Syntax

```
digit-manipulation {
    digit-transform digit-transform-name; {
        regular-expression digit-transform-rule;
        }
    }
```

Hierarchy Level [edit services convergence-services]

Description Configure digit transform rules to be used for trunk groups. A digit transform rule specifies how an outgoing called number is manipulated before it is sent to the PSTN and routed to its destination. You can use a single digit transform rule for multiple trunk groups or create unique ones to satisfy the requirements for various digit patterns.

A digit transform rule is specified as a regular expression. When a called number matches the digit pattern of a route pattern, if a digit transform rule is configured for the trunk group, then the rule is applied to the number's digits to transform it before it is sent out a trunk.

Many techniques exist for performing digit manipulation using digit transform rules. You can add digits, strip them, change them, and expand a telephone number.

You can configure the dial plan to convert telephone numbers internal to the branch to be handled by the PSTN. It is common for organizations to require employees to dial an access code, such as the digit 9, to make outside calls. Using digit manipulation, you can remove the 9 from a telephone number before sending the call to the PSTN so that the PSTN won't reject it.

It's helpful to name rules to represent what they do. For example, you might call a rule that adds a branch prefix to a telephone number "add-branch-prefix".

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

digit-transform (rule)

Syntax digit-transform *digit-transform-name*;

Hierarchy Level [edit services convergence-services digit-manipulation]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a digit transform rule to be created and used for trunk groups to manipulate the digits of called numbers to be routed to the PSTN using a trunk belonging to the trunk group. (You specify the digit transform rule name as part of a trunk group in a route pattern.)

Options *digit-transform-name*—Name of a preconfigured digit transform rule.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

digit-transform (trunk group)

Syntax digit-transform *digit-transform-name*;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-pattern *digit-pattern* trunk-group *trunk-group-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a preconfigured digit transform rule used to manipulate the digits of a called number before it is routed to the PSTN. You specify the digit transform rule name as part of a trunk group in a route pattern.

Options *digit-transform-name*—Name of a preconfigured digit transform rule.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

direct-inward-dialing

Syntax direct-inward-dialing *DID-number*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the direct inward dialing (DID) number for the station. DID allows a party who knows the internal extension of the station's telephone to dial the full seven digit number to place the call directly, bypassing the company operator or auto-attendant. Organizations can buy ranges of DID numbers from their PSTN.

Options *DID-number*—DID number to be used as the station's external telephone number.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

direct-inward-line

Syntax direct-inward–line tdm-interface *interface-name* time-slot *timeslot-number* trunk-group *trunk—group-name*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of the interface and the time slot to be used for direct inward dialing (DID) calls to the station. Specify the trunk group to be used for incoming calls. When used for a FAX station, direct inward line feature supports routing of incoming FAX calls directly to the station, bypassing the call being routed to the peer call server for handling.

Options *interface-name*—Name of the TDM interface to be used for DID calls to the station.

timeslot-number—Timeslot to be used for the line. Specify a number within the range of 0–24

trunk-group—Name of the trunk group whose trunks are to be used for incoming calls to the FAX station.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

directory

Syntax directory *directory–name*;

Hierarchy Level [edit services convergence-services features music-on-hold]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Music on hold allows for music to be played for all calls that are placed on hold. The music is played from a previously loaded file. For the file or files to be found, you must specify the directory to which you uploaded them.

Options *directory*—The directory where the files have been uploaded.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

dtmf-method (peer call server, sip template)

Syntax dtmf-method (rfc-2833 | sip-info |inband);

Hierarchy Level [edit services convergence-services station-template sip-template]
[edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the dual tone multi-frequency (DTMF) relay method for a SIP template or for the peer call server to be used when the survivable call server is in control. When the SIP template is applied to a SIP phone, the phone inherits the DTMF method.

DTMF uses eight different frequency signals sent in pairs to represent sixteen different numbers, symbols, and letters. Each tone is actually two frequencies, low and high, hence the name dual tone.

DTMF tones are generated when you press a button on a touch-tone phone. Although telephone systems are designed to carry voice signals, they must also carry other signals such as those representing telephone numbers that specify the number of the recipient of the call or a long-distance carrier, or signals that direct the network to send credit card information, for example. DTMF signalling accommodates these requirements.

After you press a button on the phone, DTMF enables dialing by identifying which key was pressed. It compresses the signal and sends it to the other party where it is decompressed. After you press a button on the phone, DTMF enables dialing by identifying which key was pressed. It compresses the signal and sends it to the other party where it is decompressed.

Options *dtmf-method*—The DTMF method to be used. The following methods are supported:

- rfc-2833
- sip-info (SIP-INFO)
- inband

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

extension (live-attendant)

Syntax extension *extension-number*;

Hierarchy Level [edit services real-time-media features auto-attendant live-attendant]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Some companies choose to provide a single number for external callers. When calls are placed to this number, they are handled by an operator (referred to as a live attendant) or rerouted to auto-attendant.

Specify the extension number of the “live-attendant” to whom calls are directed initially. When this person is unavailable to take calls at this telephone extension and the telephone rings for a specified number of times, the call is passed to auto-attendant. Some companies use a combination of auto-attendant and direct inward dialing (DID) features for external callers.

Options *extension-number*—(live-attendant). Extension number of the person acting as the live-attendant operator for the auto-attendant feature.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

extension-inherit

Syntax

```
extension-inherit {
   from-extension start-range;
   to-extension end-range;
}
```

Hierarchy Level [edit services convergence-services station-template sip-template *template-name*]

Description To configure stations for multiple SIP phones, specify the range of extensions to be used.

SIP phones that match extensions within the range, inherit the station configuration specified by the named template that includes extension-inherit parameter.

Options *start-range*—The first extension number in the range of numbers to be used for SIP phones.

end-range—The last extension number in the range to be used for SIP phones.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

extension-number (voicemail)

Syntax extension-number *extension-number*;

Hierarchy Level [edit services convergence-services features voicemail]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the extension number for users to call to retrieve their voicemail when the survivable call server is in control.

The voicemail server is the same one that is used when the peer call server provides voicemail services. In this case, however, the survivable call server accesses the voicemail server using an external PSTN connection.

Two numbers are configured to provide access to voicemail:

- The remote access number of the server.
- An extension number that users can call instead of dialing the longer remote access number. This is statement specifies that extension number.

Options *extension-number*—Voicemail extension number for users to call when the survivable call server is in control. This number corresponds to the remote access number for the voicemail server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

extension (station)

Syntax extension *extension-number*;

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the extension number for the station's telephone or fax machine. This is the number to which the media gateway (SRX Series MGW) or the survivable call server (SRX Series SCS) forwards incoming calls.

Options *extension-number*—Extension number for the station's telephone or fax machine.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

features

Syntax

```
features {
   auto-attendant {
      live-attendant {
         extension extension-number;
         hours {
            start-time start-time;
            end-time end-time;
         }
         ring-count number-of-rings;
      }
      voicemail {
      }
      music-on-hold; {
         directory directory–name;
         format (alaw | µlaw | all);
         order (alphabetical | random);
      }
      }
      guest {
   }
}
```

Hierarchy Level [edit services *convergence-services*]

Description Configure auto-attendant, music-on-hold, voicemail services, and guest features.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

format

Syntax format (alaw | ulaw | all) ;

Hierarchy Level [edit services convergence-services features music-on-hold]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Music on hold allows for music to be played for all calls that are placed on hold. The music is played from a previously uploaded file. Use this statement to specify the file formats. You can specify that one or more file formats are to be used.

Options ulaw—μ-LAW. A companding algorithm typically used in the digital telephony systems of North America and Japan. Specify ulaw if you want to use files of this format, or specify *all* to include it.

alaw—A-LAW. A companding algorithm typically used in the digital telephony systems in which signals are carried over E-1 circuits, such as Europe. Specify alaw if you want to use files of this format, or specify *all* to include it.

all—Use all supported formats.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

from (route-policy)

Syntax from;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name*]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specifies that the following trunk-group statement refers to trunks from which calls are routed. The *then* partner statement specifies either a trunk group or a peer call server to which calls are routed.

Options none

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

heartbeat-normal-interval

Syntax heartbeat-normal-interval *heartbeat-normal-interval*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the heartbeat interval to specify when the survivable call server (SRX SCS) is to send keepalive messages to check if the peer call server is reachable. If the peer call server is not reachable, the survivable call server takes control.

Options *heartbeat-normal-interval*—Interval specified in seconds.
Range: 2-8 seconds
Default: 4 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

heartbeat-survivable-interval

Syntax heartbeat-survivable-interval *heartbeat-survivable-interval*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the heartbeat interval to specify when the survivable call server is to send keepalive messages to the peer call server to determine if it is reachable and has recovered from the fault condition.

Options *heartbeat-survivable-interval*—Interval specified in milliseconds.
Range: 100-1000 ms
Default: 500 ms

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

hours

Syntax hours start-time *start-time* end-time *end-time*;

Hierarchy Level [edit services convergence-services features auto-attendant live-attendant]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the hours when the person referred to as a live attendant is available to receive calls and redirect them to the intended recipient.

Options *start-time*—The beginning time when the operator or receptionist designated as the live attendant is available to receive incoming calls.

end-time—The time when the live attendant is no longer available to receive calls.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

guest

Syntax

```
guest {
    class-of-restriction class-of-restriction-configuration;
    auto-register;
}
```

Hierarchy Level [edit services convergence-services features]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Enable the guest feature to be used for SIP stations for which there are no station configurations and that are not included in the range of SIP phones specified in the extension-inherit statement. You can also specify a class-of-restriction configuration to be used for guest SIP phones. If the default guest feature is used without class-of-restriction, then the user can only make calls and not receive them.

Options *class-of-restriction-configuration*—A class-of-restriction configuration that includes one or more policies. A policy specifies that a type of call is allowed (or denied) and that a user of the phone can make that kind of call. By default all calls except emergency and intra-branch are denied. To allow a call, you must create a policy for it.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics address

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics port

password

interval

Syntax interval *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of JUNOS Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics timeout

timeout-action

live-attendant

Syntax

```
live-attendant {
    extension extension-number;
    hours {
        start-time start-time;
        end-time end-time;
    }
    ring-count number-of-rings;
}
```

Hierarchy Level [edit services convergence-services features auto-attendant]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure information about the person who is designated as the live attendant for the auto-attendant feature. Specify the person's extension number and hours when that person is available to handle calls.

The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

media-gateway

Syntax

```
media-gateway gateway-name; {
    peer-call-server server-name;
    protocol {
        sip {
            port port-number;
            transport [udp | tcp | tls];
        }
    }
    dial-plan dial-plan-name;
    service-point zone zone-name;
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the media gateway (SRX SeriesMGW). The SRX Series MGW forwards calls from analog stations to the peer call server, for processing and routing, and from the peer call server to analog stations. It routes all emergency calls from SIP phones and analog telephones out the local PSTN, if media gateway trunks are configured, or to the peer call server, if not.

The peer call server provides call handling services and call routing for calls from SIP phones and analog telephones and fax machines. With the exception of emergency calls, calls to and from SIP phones occur directly between them and the peer call server without the media gateway interceding.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

monitor-timeout

Syntax monitor-timeout *monitor-timeout*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the duration in seconds when the peer call server must respond to keepalive messages from the survivable call server for the survivable call server to assume that it has recovered from the fault condition and is reachable and constant.

The survivable call server measures whether the peer call server has recovered based on the percent of responses it receives during this watch period. The response-threshold statement specifies the requirement.

If the peer call server meets the response requirement, the survivable call server assumes that the fault condition no longer exists, and it returns control to the peer call server. Otherwise the survivable call server continues to maintain control.

Options *monitor-timeout*—Period when the survivable call server watches the peer call server to determine if it is reachable.
Range: 5–20 seconds
Default: 16 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

music-on-hold

Syntax
```
music-on-hold; {
    directory directory–name;
    format (alaw | µlaw | all);
    order (alphabetical | random);
}
```

Hierarchy Level [edit services convergence-services features]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Music on hold allows for music to be played for all calls that are placed on hold. The music is played from a previously uploaded file. You can specify the format of the files, and, if there is one more file, the order in which files are played.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

next hop (route policy)

Syntax next-hop;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name* then route]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the *next-hop* keyword to indicate that the following trunk group statement or SIP server statement is the outgoing route hop for the call.

Options none

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

order

Syntax order (alphabetical | random);

Hierarchy Level [edit services convergence-services features music-on-hold]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Music on hold allows for music to be played from one or more previously loaded files for all calls that are placed on hold. You must first upload the files. You can use this statement to specify the order in which files are played, if there is more than one file.

Options
- alphabetical—If more than one file exists, they are played in alphabetical order.
- random—If more than one file exists, they are played randomly.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

password

Syntax password *password*;

Hierarchy Level [edit services unified-access-control infranet-controller *hostname*]

Release Information Statement introduced in Release 9.4 of JUNOS Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics ca-profile

server-certificate-subject

peer call server (definition)

Syntax

```
peer-call-server server-name; {
   description peer-call-server-description;
   address peer-call-server-address;
   protocol {
      sip {
         port port-number;
         transport [udp | tcp tls];
         }
      }
   codec codec;
   dtmf-method dtmf-method;
   pstn-access-number pstn-access-number;
   auth-id authentication-id;
   auth-password authentication-password;
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure information about the peer call server that provides call handling services and routing for the media gateway (SRX Series MGW). Although you can configure only one peer call server, you can specify a FQDN for it rather than an IP address so that multiple servers can be used. In this case, the survivable call server sends heartbeat messages to all servers to determine which ones are available. It uses the preferred server, based on the domain name services (DNS) result.

The peer call provides services including auto-attendant, caller ID, direct-inward-dialing, and so forth, for calls that the SRX Series MGW directs to it from its local analog telephones and fax machines and all emergency calls, if SRX Series MGW trunks are not configured to route emergency calls. The peer call server also processes and routes branch SIP calls without the media gateway interceding.

The survivable call server monitors the health of the peer call server in order to determine when to take control and when to return control to it.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

peer call server (media gateway)

Syntax peer-call-server *server-name*;

Hierarchy Level [edit services convergence-services media-gateway *gateway-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of the peer call server to be used to provide the media gateway's call handling and call routing services. For example, if you configured information about a peer call server called "peer-server-bostonHQ", then you would specify that name for this statement.

NOTE: When you configure the peer call server, you can specify as its address a fully-qualified domain name (FQDN) rather than an IP address as a means of specifying that multiple peer call servers are to be used. In this case, the survivable call server sends heartbeat messages to all servers to determine which ones are available. It uses the preferred server, based on the domain name services (DNS) result.

Options *server-name*—Name of the peer call server that provides call routing and call handling services for the media gateway.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

peer-proxy-server

Syntax peer-proxy-server *peer-proxy-server- name*;

Hierarchy Level edit services convergence-services trunk *trunk-name* trunk-type sip]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify a name for the peer proxy server, that is, the SIP trunk service provider.

Options *peer-proxy-server-name*—Name for the SIP trunk service provider acting as the peer proxy server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

peer call server (route policy)

Syntax peer-call-server *server-name*;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name* then route next-hop]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the name of the peer call server to which the call is to be routed. The peer call server information must have been configured already using the peer-call-server statement under convergence-services.

Options *server-name*—Reference to the peer call server to which the call is to be routed.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

permission

Syntax permission (allow | deny);

Hierarchy Level [edit services convergence-services class-of-restriction *class-of-restriction-configuration* policy *policy-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify whether a type of call is allowed or denied. When the class-of-restriction configuration containing the policy is applied to a station, the configuration's policies are enforced for that station. If a policy specifies that a type of call is allowed for a station, the person using the station's telephone can make that type of call.

By default, all classes of calls are denied except emergency and intra-branch calls.

Options allow—Permit the user to make the type of call specified by the policy. You must explicitly allow call types, apart from emergency and intra-branch calls, which are allowed by default. All other types of calls are denied by default.

deny—Prohibit the user from making the type of call specified by the policy.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

policy

Syntax

```
policy {
    name policy-name;
    permission (allow | deny);
    call-type class-of-call;
}
```

Hierarchy Level [edit services convergence-services class-of-restriction *class-of-restriction-configuration*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Define a policy for a class-of-restriction configuration that specifies whether a particular type of call is allowed or denied. You can create multiple policies for a class-of-restriction configuration. A class-of-restriction configuration can be applied to a station to enforce its policies for that station or it can be assigned to a station template.

If a policy specifies that a class of call is allowed, the call is routed, if the called number matches a digit pattern in the dial plan. For example, if a policy specifies that long-distance calls are allowed, the telephone user is allowed to make long-distance calls.

Options *policy-name*—Name of a policy.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

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 to 65535.

Use this statement when you are configuring the SRX Series device to act as a JUNOS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics interface

password

port (peer-call-server, media-gateway, survivable-call-service)

Syntax port *port-number*;

Hierarchy Level [edit services convergence-services peer-call-server *server-name* protocol sip]
[edit services convergence-services media-gateway *gateway-name* protocol sip]
[edit services convergence-services survivable-call-service *survivable-call-service-name* protocol sip]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the port number to be used as the port, or communications endpoint, for the SIP protocol . The default port number is 5060.

Options *port-number*—Port number for the SIP protocol.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

protocol (peer-call-server, media-gateway, survivable-call-service)

Syntax

```
protocol {
   sip {
      port port-number;
      transport [udp | tcp | tls];
   }
}
```

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]
[edit services convergence-services media-gateway *gateway-name*]
[edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure information for the SIP protocol specifying the port number used as its communication endpoint and the transport layer protocol (TCP, UDP, or TLS) to be used for SIP communication.

NOTE: Values configured for the media gateway and the survivable call server must match.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

pstn-access-number

Syntax pstn-access-number *pstn-access-number*;

Hierarchy Level [edit services convergence-services peer-call-server *server-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the external PSTN number for the survivable call server to use to contact the peer call server directly.

Options *pstn-access-number*—External number for the survivable call server to use to contact the peer call server.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

registration-expiry-timeout

Syntax registration-expiry-timeout *registration-expiry-timeout*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the registration expiry timeout value to specify the time after which the survivable call server drops it connections to SIP phones that are registered with it so that they can register again with the peer call server.

This parameter specifies behavior that is enacted after the survivable call server determines that the peer call server is accessible and able to provide call services for the branch.

For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Options *registration-expiry-timeout*—Time after which the survivable call server drops its connections to SIP phones after the peer call server has become available.

Usage Guidelines For configuration instructions and examples, see the JUNOS Software

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

regular-expression

Syntax regular-expression *digit-transform-rule*;

Hierarchy Level [edit services convergence-services digit-manipulation digit-transform]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify a regular expression for a digit transform rule. When a called number matches a digit pattern in the dial plan, if a digit transform rule is configured for the trunk group included in the route pattern, it is used to change the called number in some way before the call is routed to the PSTN. For example, you can create digit transform rules to transform numbers by adding digits to them, subtracting digits from the numbers, or changing the numbers. Digit transform rules can be used to prefix digits to a number and expand a telephone number.

A regular expression consists of literal text characters and special characters called *metacharacters*, which indicate or control how the text can vary in the target string.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

response-threshold

Syntax response-threshold minimum *response-threshold-percent*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Description Configure the minimum percent of responses to requests from the survivable call server that the peer call server must send during a "watch period" specified by the monitor-timeout statement before the survivable call server accepts that the peer call server is reachable, has recovered from the fault condition, and is reliable.

Options *response-threshold-keepalive*—Percent of keepalive responses from the peer call server to requests from the survivable call server.
Range: 0-100 percent, default:75 percent

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

ring-count

Syntax ring-count *number-of-rings*;

Hierarchy Level [edit services convergence-services features auto-attendant]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the number of times the telephone for the person referred to as the live attendant may ring before the call is forwarded to auto-attendant for handling. Calls are forward to auto-attendant after business hours and when the live attendant is unavailable during business hours.

When a call is directed to it, auto-attendant plays the following message:

"Welcome to Integrated Convergence Services automated attendant. Please enter your party's extension or press 1 to reach voicemail."

Options *number-of-rings*—Number of times the live attendant's telephone may ring when calls are directed to it before they are redirected to the extension number for auto-attendant.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

route pattern (dial plan)

Syntax

```
route-pattern digit-pattern; {
   call-type class–of-call; {
      trunk-group trunk-group-name; {
         preference preference-number;
         digit-transform digit-transform-name;
      }
   }
}
```

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name*]

Release Information Statement introduced in Release 9.6 of JUNOS software.

Description Configure a route pattern entry for a dial plan to specify a digit pattern against which called numbers are matched. A route pattern also includes trunk groups to be used to route calls that match the pattern.

If the route pattern contains more than one trunk group, you can include a preference number that sets a precedence for that trunk group among the others. The first trunk in the preferred trunk group is used to route a call, if it is available. If not, the next trunk is tried, and so on, in order of preference through the trunk groups.

A trunk group can also include a digit transform rule used to manipulate the called number before it is routed to the telephony service provider.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

route (route policy)

Syntax route;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name* then]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the route statement to indicate that calls are to be routed either to the peer call server or to the specified trunk group.

Options none

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

route-policy

Syntax

```
route-policy route-policy-name; {
    term term-name; {
        from; {
            trunk-group trunk-group-name;
            }
            then; {
                route;
                    next-hop;
                        peer-call-server server-name;
                        trunk-group trunk-group-name;
                    }
                }
            }
        }
```

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name*]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the name of a route policy whose additional information specifies how to route calls from one trunk to another or to a SIP peer call server. The two trunks can be different types, for example, one trunk can be an FXO trunk and the other can be an FXS trunks. When this feature is used, calls are routed through the media gateway, as opposed to originating or terminating on it or stations connected to the gateway. The routing decision is based on the incoming trunk rather than the called party number or pattern, as is the case with use of route patterns.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics ca-profile

password

service-point (survivable call server, media gateway)

Syntax service-point zone *zone-name*;

Hierarchy Level [edit services convergence-services media-gateway *media-gateway-name*]
[edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Enable the media gateway and survivable call server services for the specified zone.

Options *zone-name*–Name of the zone, as specified the JUNOS Software configuration, that the survivable call services or the media gateway is enabled for.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

sip (media gateway, peer call server, survivable call server)

Syntax

```
sip {
    port port-number;
    transport [udp | tcp | tls];
}
```

Hierarchy Level

[edit services convergence-services media-gateway *gateway-name* protocol]
[edit services convergence-services peer-call-server *server-name* protocol]
[edit services convergence-services survivable-call-service *survivable-call-service-name* protocol]

Description

Configure SIP protocol information, including the port number to be used as its communication endpoint and its transport layer protocol (TCP, UDP, or TLS). SIP protocol information configured for the media gateway must match.

Statement introduced in Release 10.0 of JUNOS Software.

Options

The remaining statements are explained separately.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level

services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

sip-template (sip)

Syntax

```
sip-template sip-template-name; {
    dtmf-method dtmf-method;
    caller-id-transmit;
    class-of-restriction class-of-restriction-configuration;
codec codec;
    extension-inherit {
        from-extension start-range;
        to-extension end-range;
    }
}
```

Hierarchy Level [edit services convergence-services station-template]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Define a SIP template to be applied to SIP stations at the local branch or to be used for SIP phones whose extension numbers match an extension in the range of numbers specified by extension-inherit, if it is configured. In this case, the template's configuration is used for the matching SIP phones.

NOTE: If you use the SIP template for a SIP station, not for the extension-inherit feature, and both it and the station configuration specify a class-of-restriction (COR) configuration, the station specification takes precedence.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

sip-timeout

Syntax sip-timeout *sip-timeout*;

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the SIP time-out parameter used by the survivable call server as the watch period during which it determines if the peer call server is no longer reachable.

The survivable call server assumes that the peer call server cannot recover from the fault condition if it does not respond to keepalive messages within this period of time. After the specified time-out period expires without response from the peer call server, the survivable call server assumes responsibility.

Options *sip-timeout*—SIP time-out period during which the peer call server must response to keepalive messages to remain in control.
Range: 16 to 120 seconds
Default: 32 seconds

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

station

Syntax

```
station station-name; {
    extension extension-number;
    class-of-restriction class-of-restriction-configuration;
    caller-id caller-id-information;
    direct-inward-dialing DID-number;
    direct-inward-line {
        tdm-interface interface-name; {
        time-slot timeslot-number;
    }
    auth-id authentication-id;
    auth-password authentication-password;
    station-type {
        sip {
            template sip-template-name;
        }
        analog {
            template analog-template-name;
            tdm-interface interface-name;
                time-slot timeslot-number;
            }
        }
    }
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure basic station information. For example, you might use the name of the person who uses the telephone as the station name. For an analog station that supports a FAX machine, you might use the name of the machine. To use a template for the station, specify the template type for the station—whether SIP or analog. Templates are configured separately.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

station-template

Syntax station-template (sip-template | analog-template)

Hierarchy Level [edit services convergence-services]

Description Specify the kind of template to be configured, whether SIP or analog.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

station-type

Syntax
```
station-type {
  sip {
    template sip-template-name;
  }
    analog {
      template analog-template-name;
      tdm-interface interface-name;
      time-slot timeslot-number;
    }
  }
```

Hierarchy Level [edit services convergence-services station *station-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the type of station to be configured, either SIP or analog.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

survivable-call-service

Syntax

```
survivable-call-service survivable-call-server-name; {
    peer-call-server server-name;
    protocol {
        sip {
            port port-number;
            transport [udp | tcp | tls]; }
        }
    }
    heartbeat-normal-interval heartbeat-normal-interval;
    sip-timeout sip-timeout;
    registration-expiry-timeout expiry-timeout;
    monitor-timeout monitor-timeout;
heartbeat-survivable-interval interval;
    response-threshold {
    minimum response-threshold-percent;
    }
    service-point {
        zone zone-name;
        }
    }
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the survivable call server component of Integrated Convergence Services. If the peer call server is unavailable and the survivable call server is configured, the survivable call server assumes control. It provides call handling services and call routing previously provided by the peer call server.

NOTE: When you configure the peer call server, you can specify a FQDN for the server address rather than an IP address so that multiple servers can be used. In this case, the survivable call server sends heartbeat messages to all servers to determine which ones are available. It uses the preferred server, based on the domain name services (DNS) result.

There are many reasons for the peer call server to become unreachable. For example, there could be a disconnected cable, a congested network, routing problems, transport level problems or a denial-of-service attack on the application server hosting the peer call server.

While it is in control, the survivable call server monitors the health of the peer call server to determine if it has become reachable. To determine if the peer call server has recovered from the fault condition that caused it to become unreachable, the survivable call server relies on a set of keepalive parameters and timers.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

tdm-interface (analog station)

Syntax tdm-interface *interface-name*;

Hierarchy Level [edit services convergence-services station *station-name* station-type analog]

Description Specify the name of a preconfigured FXS, FXO, or T1 interface to be used for the specified analog station.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

tdm-interface (direct-inward-line)

Syntax tdm-interface *interface-name*;
[edit services convergence-services station *station-name* direct-inward-line]

Hierarchy Level [edit services convergence-services]

Description Specify the name of a preconfigured FXS interface to be used for direct-inward-dialing (DID) calls to the station. DID allows a party who knows the internal extension of the station's telephone to dial that seven digit number to place the call directly.

Options *interface-name*—Name of the FXS interface to be used.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

template (analog)

Syntax template *analog-template-name*;

Hierarchy Level [edit services convergence-services station *station-name* station-type analog]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a preconfigured analog template to assign to the specified analog station. The station inherits the template's parameters.

Options *analog-template-name*—Name of a preconfigured analog template.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

template (sip)

Syntax template *sip-template-name*;

Hierarchy Level [edit services convergence-services station *station-name* station-type sip]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of a preconfigured SIP template to assign to the specified SIP station. The station inherits the template's parameters.

Options *sip-template-name*—Name of a preconfigured SIP template.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

term (route policy)

Syntax term *term-name*;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name*]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the name of a term to distinguish it from other terms belonging to the same policy.

Options *term-name*—Name of a term contained in the policy.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

then

Syntax then;

Hierarchy Level [edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name*]

Release Information Statement introduced in Release 10.0 of JUNOS software.

Description Specify the *then* keyword to indicate that calls are to be routed to a trunk group or to a peer call server, as specified by the following statement. Its partner statement *from* indicates from which trunk group the call is routed.

Options none

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

timeout

Syntax timeout *seconds*;

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of JUNOS Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS 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 Enforcer connects to one at a time, failing over to other Infranet Controllers in the cluster as required.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics interval

timeout-action

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 Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS 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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Topics interval

timeout

traceoptions

Syntax

```
traceoptions {
   flag [ (ipc | config | connect | all) ];
}
```

Hierarchy Level [edit services unified-access-control]

Release Information Statement introduced in Release 9.4 of JUNOS Software.

Description Define Unified Access Control (UAC) tracing options.

Use this statement when you are configuring the SRX Series device to act as a JUNOS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS 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 configurations required for UAC enforcement such as zones, policies, and interfaces.
- connect—Trace communications between the JUNOS 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).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

transport (survivable-call-service, media-gateway, peer-call-server)

Syntax transport [udp | tcp | tls];

Hierarchy Level [edit services convergence-services survivable-call-service *survivable-call-service-name* protocol sip]
[edit services convergence-services media-gateway *gateway-name* protocol sip]
[edit services convergence-services peer-call-server *server-name* protocol sip]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the Transport Layer Protocol to be used for the SIP session. You can specify UDP, which carries messages that could be larger than the IP network's maximum transmission unit (MTU) TCP, which can carry larger messages than UDP and provide reliability and congestion control, or TLS, which provides for secure data delivery at the transport layer..

Options UDP—User Datagram Protocol. A single UDP packet carries a SIP request or response. SIP messages could be larger than the IP's MTU size. SIP does not support fragmentation, so UDP SIP messages must be smaller than the MTU size if you use UDP. SIP does not support fragmentation.

TCP—Transport Control Protocol. Because TCP can support messages of arbitrary size, it supports larger messages and provides reliability and congestion control.

TLS—Transport Layer Security, which provides for security and data integrity of communications over the Internet Protocol (IP).

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

trunk

Syntax

```
trunk trunk-name; {
   trunk-type {
      fxo {
         tdm-interface interface-name;
      }
      fxs {
         tdm-interface interface-name;
      }
      sip sip-trunk-name {
         peer-proxy-server peer-proxy-server- name;
            address [fqdn | ipv4–address];
               auth-id [authentication-id];
               auth-password[authentication-password];
               codec [ G711–A | G711–MU | G729AB];
               dtmf-method [inband | rfc-2833| sip-info];
               port port-number;
               transport [ tcp | tls | udp];
               description description;
            }
      }
   }
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure an FXS, FXO, or SIP trunk.

For FXS and FXO trunks including the type and name of the TDM interface to be used for it. Trunks are used by the media gateway and the survivable call server to access the local PSTN. Trunks are added to trunk groups, which, in turn, are used within the route patterns of a dial plan. The media gateway dial plan and the survivable call server dial plan can refer to and use the same trunks. You can define trunks for FXO and FXS TDM interfaces.

Options The remaining statements are explained separately.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

trunk-group (definition)

Syntax

```
trunk-group trunk-group-name; {
    trunk trunk-name;
}
```

Hierarchy Level [edit services convergence-services]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure a trunk group composed of one or more trunks. Trunks are configured discretely outside a trunk group and then added to it. For a trunk group composed of multiple trunks, specify the trunks in order of precedence in which they should be used to route a call.

A trunk group is referred to in a route pattern entry of a dial plan. When a called number matches the digit pattern of a route pattern, the system attempts to route the call using the first trunk specified in the preferred trunk group of that route pattern. If the first trunk is busy, then the second trunk is tried, and so on, in order through the list of trunks configured for the trunk group.

Trunk groups are reusable across route patterns of a dial plan.

Options *trunk-group-name*—Name of the trunk group.

trunk-name—Name of the trunk to be added to the trunk group.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

trunk-group (route-pattern, route-policy)

Syntax

```
trunk-group trunk-group-name; {
    preference preference-number;
    digit-transform digit-transform-name;
}
```

Hierarchy Level

[edit services convergence-services dial-plan *dial-plan-name* route-pattern *digit-pattern*]

[edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name* from]

[edit services convergence-services dial-plan *dial-plan-name* route-policy *route-policy-name* term *term-name* then route next-hop]

Description

Trunk Groups for Route Patterns

For route patterns, specify the name of the trunk group to be added to it. If the route pattern contains more than one trunk group, you can assign each trunk group a preference number. If no preference number is assigned, trunk groups are tried in the order in which you assigned them to the route pattern. Optionally, specify a digit transform to be used to transform the called number before it is routed to the telephony service provider.

Trunk groups are reusable across route patterns of a dial plan.

Trunk Groups for Route Policies

For a route policy *from* keyword, specify the trunk group from which a call is routed either to another trunk group or to a SIP peer call server.

For the route policy's *next-hop* partner statement, specify the trunk group to which a call is routed.

If the route pattern contains more than one trunk group, you can assign each trunk group a preference number. If no preference number is assigned, trunk groups are tried in the order in which you assigned them to the route policy. Optionally, specify a digit transform to be used to transform the called number before it is routed to the telephony service provider.

Trunk groups are reusable across route policies of a dial plan.

Using Trunk Groups Within Dial Plans

A route pattern or route policy can have multiple trunk groups associated with it. Each trunk group included in a route pattern or route policy can specify a preference number (low-order number takes precedence) that indicates which trunk group is used first.

- If you use preference numbers, trunks within the trunk group with the highest preference (lowest number) are tried first.

- If no preference number is assigned to the trunk groups, they are used in the order in which you add them to the route pattern.

Integrated Convergence Services tries to route the call using the first trunk in the preferred trunk group. If that trunk is used for a call, the next trunk in that trunk group is tried, and so on until an available trunk is identified.

If no trunk is available in the first trunk group of the route pattern or the route policy, then the trunk group with the next highest preference is tried. Its first trunk is tried. If the first trunk is busy with a call, then the next trunk of that trunk group is tried until an available trunk is identified and the call is routed.

If all trunks of the trunk groups are unavailable to route the call, the following message is played:

"We are sorry. All circuits are busy now. Please try again later."

Options

trunk-group-name—Name of the trunk group.

preference-number—Order in which the trunk group should be used. Lowest number indicates highest preference.

digit-transform-name—Name of a digit transform to be used for trunks in this trunk group.

Usage Guidelines

For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level

services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

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 Software.

Description Use this statement to configure the SRX Series device to act as a JUNOS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

voice-activity-detection

Syntax voice-activity-detection (disable);

Hierarchy Level [edit services convergence-services station-template analog-template *analog-template-name*]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure the voice activity detection (VAD) feature for the specified analog station template to either disable or enable it for all phones that the station template is applied to. By default, VAD is enabled

For VoIP communication across the IP WAN, VAD detects the presence of speech in an audio signal. VAD can reduce bandwidth usage, computational processing, and network traffic by sending audio packets only if speech is detected.

NOTE: Because people are uncomfortable with the total silence that remains during phone conversations when VAD is enabled and no one is speaking, comfort noise generation is often used with VAD to provide familiar background sound.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

voicemail

Syntax

```
voicemail
  {
    extension-number extension-number;
    remote-access-number remote-access-number;
  }
```

Hierarchy Level [edit services convergence-services features]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Configure access to the voicemail system to be used when the survivable call server is in control. Specify the PSTN remote access number of the voicemail server. To make it easier for users to dial into voicemail, configure an extension number that they can use.

NOTE: Because voicemail is accessed through the PSTN, the user might be prompted for a user ID and password.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

zone (media-gateway, survivable-call-service)

Syntax zone *zone-name;*

Hierarchy Level [edit services convergence-services media-gateway *media-gateway-name* service-point]
[edit services convergence-services survivable-call-service *survivable-call-service-name* service-point]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

Description Specify the name of the zone for which you are enabling either the media gateway or the survivable call server. The zone is created using the JUNOS Software configuration. You create a zone and bind interfaces to it to associate segments of a network with it.

Options *zone-name*—Name of the zone for which the media gateway or the survivable call server is enabled. For example, if you are enabling the media gateway services for the branch zone, specify the zone name, such as *sf-branch-zone*, or *trusted*, or *trusted* and *untrusted* if using generic terms. The zone must have previously been created for that department, in which case all of the interfaces on the Loki210 composing the zone must have been bound to the zone.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Integrated Convergence Services Configuration and Administration Guide*.

Required Privilege Level services—To view this statement in the configuration.
services–control—To add this statement to the configuration.

Chapter 20

SNMP Hierarchy and Statements

This chapter presents the complete snmp configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

Use the statements in the snmp configuration hierarchy to configure the Simple Network Management Protocol (SNMP) for monitoring device operation and performance. For configuration instructions, see the *JUNOS Software Administration Guide*.

For information about snmp statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS Network Management Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter contains the following sections:

- SNMP Configuration Statement Hierarchy on page 857

SNMP Configuration Statement Hierarchy

To configure SNMP, use the following statements at the [edit snmp] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the snmp hierarchy are shown in normal font and are documented in the *JUNOS Network Management Configuration Guide*.

```
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);
}
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  {
                    group  group-name ;
                }
            }
        }
    }
}
view  view-name  {
    oid  oid-name  {
        <exclude | include>;
    }
}
}
}
```

authorization

Syntax authorization (read-only | read-write);

Hierarchy Level [edit snmp community *community-name*]

Release Information Statement modified in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Chapter 21

System Hierarchy and Statements

This chapter presents the complete system configuration hierarchy available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Where applicable, the chapter also provides a summary for each statement in the hierarchy that is exclusive to J Series and SRX Series devices. Statement summaries are organized alphabetically.

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; and properties of the device's auxiliary and console ports. For configuration instructions, see the *JUNOS Software Security Configuration Guide* and the *JUNOS Software Administration Guide*.

For information about system statements that are not explained here—statements that are shared across Juniper Networks devices—see the *JUNOS System Basics Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

This chapter includes the following sections:

- System Configuration Statement Hierarchy on page 863

System Configuration Statement Hierarchy

To configure system properties, use the following statements at the [edit system] hierarchy level. Statements exclusively for J Series and SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

Shared JUNOS statements in the system hierarchy are shown in normal font and are documented in the *JUNOS System Basics Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.

```
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 ;
        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;
    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 ;
      }
    }
}
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;
    }
  }
  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 ;
        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 ;
            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 );
   }
```

firewall-authentication-service

Syntax firewall-authentication-service (enable | disable);

Hierarchy Level [edit system processes]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable or disable the firewall authentication service process.

Options enable—Start the firewall authentication service process.

disable—Stop the firewall authentication service process.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

network-security

Syntax network-security (enable | disable);

Hierarchy Level [edit system processes]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

Description Enable or disable the network security process on the device.

Options enable—Start the network security process.

disable—Stop the network security process.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Port

See the following sections:

- port (reverse ssh)
- port (reverse telnet)

port (reverse ssh)

Syntax reverse ssh port *5000*

Hierarchy Level [edit system services reverse ssh port 5000]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Administration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

port (reverse telnet)

Syntax reverse telnet port *6000*

Hierarchy Level [edit system services reverse telnet port 6000]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Administration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

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 Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Administration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

reverse ssh

Syntax reverse ssh

Hierarchy Level [edit system services reverse ssh]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Administration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

reverse telnet

Syntax reverse telnet

Hierarchy Level [edit system services reverse telnet]

Release Information Statement introduced in Release 9.6 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *JUNOS Administration Guide*.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

system-generated-certificate

Syntax system-generated-certificate;

Hierarchy Level [edit system services web-management https]

Description Automatically generated self-signed certificate

Usage Guidelines For configuration instructions and examples, see the *JUNOS Software Security Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

traceoptions

See the following sections:

- traceoptions (General Authentication Service) on page 880
- traceoptions (WAN Acceleration) on page 882

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 Software.

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.

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 Software.

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

Usage Guidelines For configuration instructions and examples, see the *WXC Integrated Services Module Installation and Configuration Guide*.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

wan-acceleration

Syntax wan-acceleration (enable | disable);

Hierarchy Level [edit system processes]

Release Information Statement introduced in Release 8.5 of JUNOS Software.

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.

Usage Guidelines For configuration instructions and examples, see the *WXC Integrated Services Module Installation and Configuration Guide*.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Chapter 22
Wlan Hierarchy and Statements

This chapter presents the complete wlan configuration hierarchy available on SRX210, SRX240, and SRX650 Services Gateways running JUNOS software. The chapter also provides a summary for each statement in the hierarchy. Statement summaries are organized alphabetically.

Use the statements in the wlan configuration hierarchy to configure wireless LAN features on the device. For configuration instructions, see the *JUNOS Software WLAN Configuration and Administration Guide*.

This chapter contains the following sections:

- [edit wlan] Configuration Statement Hierarchy on page 885

[edit wlan] Configuration Statement Hierarchy

To configure security rules, actions, and zones, use the following statements at the [edit wlan] hierarchy level. Statements exclusively for SRX Series devices running JUNOS Software are shown in bold font and are documented in this chapter.

```
wlan {
    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;
            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);
    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;
        }
    }
  }
}
```

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 {
            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);
```

```
            }
          }
          ssid ssid;
          vlan vlan-id;
        }
      }
    }
```

Hierarchy Level [edit wlan]

Release Information Statement introduced in Release 10.0 of JUNOS Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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
- 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.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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.

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 Software.

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.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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-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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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.

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;
            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 Software.

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 Software.

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 Software.

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.

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 Software.

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.

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 Software.

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.

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 Software.

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 Software.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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.

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 Software.

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 to 65535. 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 Software.

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 Software.

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.

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 Software.

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 Software.

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 Software.

Description Configure virtual access point for an access point radio.

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 Software.

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 Software.

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.

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 Software.

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 Software.

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.

Part 2
Operational Commands

- Clear Commands on page 935
- Request Commands on page 1005
- Restart Commands on page 1037
- Show Commands on page 1039

Chapter 23

Clear Commands

This chapter presents the clear operational commands available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Use the clear operational commands to clear software processes on the device. Operational commands are organized alphabetically.

The commands shown in this chapter are exclusive to J Series and SRX Series devices. For information about clear commands that are not explained here—commands that are shared across Juniper Networks devices—see the*JUNOS System Basics and Services Command Reference*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

clear chassis cluster control-plane statistics

Syntax clear chassis cluster control-plane statistics

Release Information Command introduced in Release 9.3 of JUNOS Software.

Description Clear the control plane statistics of a chassis cluster.

Required Privilege Level clear

Related Topics show chassis cluster control-plane statistics

List of Sample Output clear chassis cluster control-plane statistics on page 936

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
```

clear chassis cluster data-plane statistics

Syntax clear chassis cluster data-plane statistics

Release Information Command introduced in Release 9.3 of JUNOS Software.

Description Clear the data plane statistics of a chassis cluster.

Required Privilege Level clear

Related Topics show chassis cluster data-plane statistics

List of Sample Output clear chassis cluster data-plane statistics on page 937

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 Software.

Description Clear the failover count of all redundancy-groups.

Required Privilege Level clear

Related Topics request chassis cluster failover node

request chassis cluster failover reset

show chassis cluster status

List of Sample Output show chassis cluster status on page 938
clear chassis cluster failover-count on page 938
show chassis cluster status on page 938

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
  node1           10        secondary    no       no
```

clear chassis cluster statistics

Syntax clear chassis cluster statistics

Release Information Command introduced in Release 9.3 of JUNOS Software.

Description Clear the control plane and data plane statistics of a chassis cluster.

Required Privilege Level clear

Related Topics show chassis cluster statistics

List of Sample Output clear chassis cluster statistics on page 939

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
```

clear esis adjacency

Syntax clear esis adjacency
<instance *instance-name*>
<interface *interface-name*)>
<*neighbor*>

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics show esis adjacency

List of Sample Output clear esis adjacency on page 940

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 Software.

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 Topics show esis statistics

List of Sample Output clear esis statistics on page 941

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
```

clear network-access requests pending

Syntax clear network-access requests pending
<index *index-number* >

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics show network-access requests pending

List of Sample Output clear network-access requests pending on page 942

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
```

clear gtp tunnels

Syntax clear security gprs gtp tunnel <all | *identifier*>

Release Information Command introduced in Release 10.0 of JUNOS Software.

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

clear network-access requests statistics

Syntax clear network-access requests statistics

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Clear general authentication statistics for the configured authentication type.

Required Privilege Level clear

Related Topics authentication-order

show network-access requests statistics

List of Sample Output clear network-access requests statistics on page 944

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 Software.

Description Delete the node secret file for the SecurID authentication type.

Required Privilege Level clear

Related Topics configuration-file

securid-server

show network-access securid-node-secret-file

List of Sample Output clear network-access securid-node-secret-file on page 945

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics h323

show security alg h323 counters

List of Sample Output clear security alg h323 counters on page 946

Output Fields This command produces no output.

clear security alg h323 counters

```
user@host> clear security alg h323 counters
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics mgcp

show security alg mgcp calls

List of Sample Output clear security alg mgcp calls on page 947

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics mgcp

show security alg mgcp counters

List of Sample Output clear security alg mgcp counters on page 948

Output Fields This command produces no output.

clear security alg mgcp counters

```
user@host> clear security alg mgcp counters
```

clear security alg msrpc portmap

Syntax clear security alg msrpc portmap

Release Information Command introduced in Release 9.0 of JUNOS Software.

Description Clear information about Microsoft's implementation of the remote procedure call (MSRPC) mapping table.

Required Privilege Level clear

Related Topics msrpc

show security alg msrpc

List of Sample Output clear security alg msrpc portmap on page 949

Output Fields This command produces no output.

clear security alg msrpc portmap

```
user@host> clear security alg msrpc portmap
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sccp

show security alg sccp calls

List of Sample Output clear security alg sccp calls on page 950

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sccp

show security alg sccp counters

List of Sample Output clear security alg sccp counters on page 951

Output Fields This command produces no output.

clear security alg sccp counters

```
user@host> clear security alg sccp counters
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

show security alg sip calls

List of Sample Output clear security alg sip calls on page 952

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

show security alg sip counters

List of Sample Output clear security alg sip counters on page 953

Output Fields This command produces no output.

clear security alg sip counters

```
user@host> clear security alg sip counters
```

clear security alg sunrpc portmap

Syntax clear security alg sunrpc portmap

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Clear Sun Microsystem remote procedure call (SUNRPC) mapping table information.

Required Privilege Level clear

Related Topics sunrpc

show security alg sunrpc portmap

List of Sample Output clear security alg sunrpc portmap on page 954

Output Fields This command produces no output.

clear security alg sunrpc portmap

```
user@host> clear security alg sunrpc portmap
```

clear security alg sunrpc portmap

Syntax clear security alg sunrpc portmap

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Clear Sun Microsystem remote procedure call (SUNRPC) mapping table information.

Required Privilege Level clear

Related Topics sunrpc

show security alg sunrpc portmap

List of Sample Output clear security alg sunrpc portmap on page 955

Output Fields This command produces no output.

clear security alg sunrpc portmap

```
user@host> clear security alg sunrpc portmap
```

clear security datapath-debug counter

Syntax clear security datapath-debug counters

Release Information Command introduced in Release 10.0 of JUNOS Software.

Description Clear all data path-debugging counters.

Required Privilege Level clear

Related Topics show security datapath-debug capture

show security datapath-debug counter

List of Sample Output clear security datapath-debug counters on page 956

Output Fields This command produces no output.

clear security datapath-debug counters

```
user@host> clear security datapath-debug counters
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics
firewall-authentication (Security)

show security firewall-authentication history

List of Sample Output
clear security firewall-authentication history on page 957
clear security firewall-authentication history node 1 on page 957

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

show security firewall-authentication history address

List of Sample Output clear security firewall-authentication history address 100.0.0.1 on page 958
clear security firewall-authentication history address 100.0.0.1 node 1 on page 958

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:
--------------------------------------------------------------------------
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

show security firewall-authentication history identifier

List of Sample Output clear security firewall-authentication history identifier 2 on page 959
clear security firewall-authentication history identifier 2 node 1 on page 959

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security firewall-authentication users

List of Sample Output clear security firewall-authentication users on page 960
clear security firewall-authentication users node 1 on page 960

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:
--------------------------------------------------------------------------
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security firewall-authentication users address

List of Sample Output clear security firewall-authentication users address 100.0.0.1 on page 961
clear security firewall-authentication users address 100.0.0.1 node 1 on page 961

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security firewall-authentication users identifier

List of Sample Output clear security firewall-authentication users identifier 2 on page 962
clear security firewall-authentication users identifier 2 node 1 on page 962

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:
--------------------------------------------------------------------------
```

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Clear all currently active security sessions on the device.

Options 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 Topics show security flow session

List of Sample Output clear security flow session all on page 963
clear security flow session all node 0 on page 963

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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.

Required Privilege Level clear

Related Topics show security flow session application

List of Sample Output clear security flow session application dns on page 965
clear security flow session application dns node 0 on page 965

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
```

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 Ssoftware; node options added in Release 9.0 of JUNOS Software.

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 Topics show security flow session destination-port

List of Sample Output clear security flow session destination-port 1 on page 966
clear security flow session destination-port 1 node 0 on page 966

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Clear sessions that match this destination IPv4 prefix or address.

Options *destination-IP-prefix* —Destination IPv4 prefix or address.

node—(Optional) For chassis cluster configurations, clear sessions that match the IPv4 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 Topics show security flow session destination-prefix

List of Sample Output clear security flow session destination-prefix 100.0.0.1 on page 967
Clear security flow session destination-prefix 100.0.0.1 node 0 on page 967

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

```
user@host> 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 100.0.0.1 node 0

```
user@host> clear security flow session destination-prefix 100.0.0.1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

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 Software; node options added in Release 9.0 of JUNOS Ssoftware.

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 Topics show security flow session interface

List of Sample Output clear security flow session interface ge-0/0/0.0 on page 968
clear security flow session interface ge/0/0.0 node 0 on page 968

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 Software; node options added in Release 9.0 of JUNOS Software.

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

Related Topics show security flow session protocol

List of Sample Output

clear security flow session protocol pim on page 970
clear security flow session protocol 0 on page 970

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security flow session resource-manager

List of Sample Output clear security flow session resource-manager on page 971
clear security flow session resource-manager node 0 on page 971

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Clear the session with the specific identifier.

Options *session-identifier* —Number from 1 through 4294967295 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 Topics show security flow session session-identifier

List of Sample Output clear security flow session session-identifier 1 on page 972
clear security flow session session-identifier 1 node 0 on page 972

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Clear each session that uses the specified source port.

Options *source-port-number* —Number that identifies the source port.

Range: 1 through 65535

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 Topics show security flow session source-port

List of Sample Output clear security flow session source-port 1 on page 973
clear security flow session source-port 1 node 0 on page 973

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Clear sessions that match the source prefix.

Options *source-prefix-number* —Source IPv4 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 Topics show security flow session source-prefix

List of Sample Output clear security flow session source-prefix 100.0.0.1 on page 974
clear security flow session source-prefix 100.0.0.1 node 0 on page 974

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 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 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 Software.

Description Clear IDP application system cache.

Required Privilege Level clear

Related Topics application-system-cache

show security idp application-identification application-system-cache

List of Sample Output clear security idp application-identification application-system-cache on page 975

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
```

clear security idp attack table

Syntax clear security idp attack table

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Clear details of the IDP attack table.

Required Privilege Level clear

Related Topics attacks

show security idp attack table

List of Sample Output clear security idp attack table on page 976

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 Software.

Description Reset all the application identification counter values.

Required Privilege Level clear

Related Topics application (AppDDoS)

show security idp counters application-identification

List of Sample Output clear security idp counters application-identification on page 977

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
```

clear security idp counters dfa

Syntax clear security idp counters dfa

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Reset all the DFA counter values.

Required Privilege Level clear

Related Topics show security idp counters dfa

List of Sample Output clear security idp counters dfa on page 978

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 Software.

Description Reset all the IDP flow-related counter values.

Required Privilege Level clear

Related Topics flow (IDP)

show security idp counters flow

List of Sample Output clear security idp counters flow on page 979

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
```

clear security idp counters ips

Syntax clear security idp counters ips

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Reset all the ips counter values.

Required Privilege Level clear

Related Topics ips

show security idp counters ips

List of Sample Output clear security idp counters ips on page 980

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 Software.

Description Reset all the IDP log counter values.

Required Privilege Level clear

Related Topics event-rate

show security idp counters log

List of Sample Output clear security idp counters log on page 981

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
```

clear security idp counters packet

Syntax clear security idp counters packet

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Reset all the IDP packet counter values.

Required Privilege Level clear

Related Topics show security idp counters packet

List of Sample Output clear security idp counters packet on page 982

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 Software.

Description Reset all the IDP policies counter values.

Required Privilege Level clear

Related Topics show security idp counters policy-manager

List of Sample Output clear security idp counters policy-manager on page 983

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
```

clear security idp counters tcp-reassembler

Syntax clear security idp counters tcp-reassembler

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Reset all the TCP reassembler counter values.

Required Privilege Level clear

Related Topics re-assembler

show security idp counters tcp-reassembler

List of Sample Output clear security idp counters tcp-reassembler on page 984

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 Software.

Description Clear all the entries stored in the SSL session ID cache.

Required Privilege Level clear

Related Topics show security idp ssl-inspection session-id-cache

List of Sample Output clear security idp ssl-inspection session-id-cache on page 985

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
```

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 Software.

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 Topics respond-bad-spi

List of Sample Output clear security ike respond-bad-spi-count on page 986
clear security ike respond-bad-spi-count gateway-name1 on page 986

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* >
<fpc *slot-number*>
<index*SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pics*lot-number*>

Release Information
Command introduced in Release 8.5 of JUNOS Software; fpc, pic, and kmd-instance options added in Release 9.3 of JUNOS Software.

Description
Clear information about the current Internet Key Exchange (IKE) security associations.

Options
none—Clear all IKE security associations.

peer-address —(Optional) Clear IKE security associations for the destination peer at this IP address.

fpc *slot-number* —Specific to SRX Series devices. Clear information about existing IKE SAs in this particular Flexible PIC Concentrator (FPC) slot.

index *SA-index-number* —(Optional) Clear the IKE security association with this index number.

kmd-instance—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (daemon) (KMD) identified by the 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 particular PIC slot.

Required Privilege Level
clear

Related Topics
show security ike security-associations

List of Sample Output
clear security ike security-associations on page 987
clear security ike security-associations 1.1.1.2 on page 988
clear security ike security-associations index 8 on page 988
clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series devices) on page 988

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

```
user@host> clear security ike security-associations 1.1.1.2
```

clear security ike security-associations index 8

```
user@host> clear security ike security-associations index 8
```

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*

Release Information
Command introduced in Release 8.5 of JUNOS Software; fpc, pic, and kmd-instance options added in Release 9.3 of JUNOS Software.

Description
Clear information about IPsec security associations.

Options
none—Clear all IPsec security associations.

fpc *slot-number* —Specific to SRX Series devices. Clear information about existing IPsec SAs in this particular Flexible PIC Concentrator (FPC) slot.

index *SA-index-number* —(Optional) Clear the IPsec security association with this index number.

kmd-instance—Specific to SRX Series devices. Clear information about existing IPsec SAs in the key management process (daemon) (KMD) identified by the 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 particular PIC slot.

Required Privilege Level
clear

Related Topics
show security ipsec security-associations

List of Sample Output
clear security ipsec security-associations on page 989
clear security ipsec security-associations index 8 on page 989

Output Fields
This command produces no output.

clear security ipsec security-associations

```
user@host> clear security ipsec security-associations
```

clear security ipsec security-associations index 8

```
user@host> clear security ipsec security-associations index 8
```

clear security ipsec statistics

Syntax clear security ike statistics
<fpc *slot-number*>
<index *SA-index-number*>
<pic *slot-number*>

Release Information Command introduced in Release 8.5 of JUNOS Software; fpc and pic options added in Release 9.3 of JUNOS Software.

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 SAs in this particular Flexible PIC Concentrator (FPC) slot.

index *SA-index-number* —(Optional) Clear the IPsec statistics for the security association with this index number.

pic *slot-number* —Specific to SRX Series devices. Clear statistics about existing IPsec SAs in this particular PIC slot.

Required Privilege Level clear

Related Topics show security ipsec statistics

List of Sample Output clear security ipsec statistics on page 990
clear security ipsec statistics index 1 on page 990
clear security ipsec statistics fpc 5 pic 0 (SRX Series devices) on page 990

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security nat incoming-table

List of Sample Output clear security nat incoming-table on page 991

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 Software.

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 Topics show security nat source persistent-nat-table

List of Sample Output clear security nat source persistent-nat-table all on page 992

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
```

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 Software.

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 Topics show security pki certificate-request

List of Sample Output clear security pki key-pair all on page 993

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 Software.

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 Topics show security pki local-certificate

request security pki local-certificate generate-self-signed

List of Sample Output clear security pki local-certificate all on page 994
clear security pki local-certificate system-generated on page 994

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
```

clear security policies statistics

Syntax clear security policies statistics

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Clear statistics for security policies configured on the device.

Required Privilege Level clear

Related Topics show security policies

List of Sample Output clear security policies statistics on page 995

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 Software.

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 Topics show security screen statistics

List of Sample Output clear security screen statistics node 0 on page 996

Output Fields This command produces no output.

clear security screen statistics node 0

```
user@host> clear security screen statistics node 0
```

clear security screen statistics interface

Syntax clear security screen statistics interface *interface-name*

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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 Topics show security screen statistics

List of Sample Output clear security screen statistics interface fab0 on page 997
clear security screen statistics interface fab0 node 0 on page 997

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 Software; node options added in Release 9.0 of JUNOS Ssoftware.

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 Topics show security screen statistics

List of Sample Output clear security screen statistics zone abc node all on page 998
clear security screen statistics node 0 zone my-zone on page 998

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.
```

clear security utm anti-spam statistics

Syntax clear security utm anti-spam statistics

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Clear antispam statistics information.

Required Privilege Level clear

Related Topics show security utm anti-spam statistics

show security utm anti-spam status

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 Software.

Description Clear antivirus statistics information.

Required Privilege Level clear

Related Topics show security utm anti-virus statistics

show security utm anti-virus status

request security utm anti-virus juniper-express-engine

request security utm anti-virus kaspersky-lab-engine

Output Fields This command produces no output.

clear security utm antivirus statistics

```
user@host> clear security utm anti-virus statistics
```

clear security utm content-filtering statistics

Syntax clear security utm content-filtering statistics

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Clear content-filtering statistics information.

Required Privilege Level clear

Related Topics show security utm content-filtering statistics

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 Software.

Description Clear UTM session information.

Required Privilege Level clear

Related Topics show security utm session

show security utm status

Output Fields This command produces no output.

clear security utm session

```
user@host> clear security utm session
```

clear security utm web-filtering statistics

Syntax clear security utm web-filtering statistics

Release Information Command introduced in Release 9.5 of JUNOS Ssoftware.

Description Clear web filtering statistics information.

Required Privilege Level clear

Related Topics show security utm web-filtering statistics

show security utm web-filtering status

Output Fields This command produces no output.

clear security utm web-filtering statistics

```
user@host> clear security utm web-filtering statistics
```

Chapter 24

Request Commands

This chapter presents the request operational commands available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. 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.

The commands shown in this chapter are exclusive to J Series and SRX Series devices. For information about request commands that are not explained here—commands that are shared across Juniper Networks device—see the *JUNOS System Basics and Services Command Reference*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

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 Software.

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 Topics clear chassis cluster failover-count

request chassis cluster failover reset

show chassis cluster status

List of Sample Output request chassis cluster failover node 0 redundancy-group 1 on page 1006

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 Software.

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 Topics
clear chassis cluster failover-count

request chassis cluster failover node

show chassis cluster status

List of Sample Output
request chassis cluster failover reset redundancy-group 0 on page 1007

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
```

request modem wireless activate iota

Syntax request modem wireless activate iota *interface-name*

Release Information Command introduced in Release 9.5 of JUNOS Software.

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 Software.

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 Topics show modem wireless interface network

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
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 Software.

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.
```

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 Software.

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 Topics request modem wireless gsm sim-unlock

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 Software.

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 Topics request modem wireless gsm sim-unblock

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
```

request security datapath-debug capture start

Syntax request security datapath-debug capture start

Release Information Command introduced in Release 10.0 of JUNOS Software.

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 Software.

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 succesfully stopped, use show security datapath-debug
capture to view
```

request security idp security-package download

Syntax

request security idp security-package download
<check-server>
<full-update>
<policy-templates>
<status>
<version *version-number* >

Release Information

Command introduced in Release 9.2 of JUNOS Software.

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.

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.

Required Privilege Level

maintenance

Related Topics

show security idp active-policy

show security idp security-package-version

List of Sample Output

request security idp security-package download on page 1016
request security idp security-package download policy-templates on page 1016
request security idp security-package download version 1151 full-update on page 1016

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

```
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)
```

download version 1151 full-update

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 Software.

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.

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 Topics
show security idp active-policy

show security idp security-package-version

List of Sample Output
request security idp security-package install on page 1018
request security idp security-package install status on page 1018

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

```
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.
```

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 Software.

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 Topics show security idp ssl-inspection key

List of Sample Output request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted on page 1019
request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted on page 1019
request security idp ssl-inspection key add key3 file /var/tmp/norm.key on page 1020
request security idp ssl-inspection key add key1 server 1.1.0.1 on page 1020
request security idp ssl-inspection key add key1 server 1.1.0.2 on page 1020

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

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
```

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 Software.

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 Topics show security idp ssl-inspection key

List of Sample Output
request security idp ssl-inspection key delete on page 1021
request security idp ssl-inspection key delete key1 on page 1021
request security idp ssl-inspection key delete key2 server 2.2.0.1 on page 1021

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

Number of keys 0, server 1 deleted
```

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 Software.

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 Topics ca-profile

show security pki ca-certificate

List of Sample Output request security pki ca-certificate verify ca-profile ca1 (CRL downloaded) on page 1022
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded) on page 1022

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 Software.

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 Topics clear security pki local-certificate

show security pki local-certificate

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 1024

Output Fields When you enter this command, you are provided feedback on the status of your request.

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 Software.

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 1025
request security pki local-certificate verify certificate bme1 (downloaded) on page 1025

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
```

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 Software.

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 Topics request security utm anti-virus kaspersky-lab-engine

clear security utm antivirus statistics

show security utm anti-virus statistics

show security utm anti-virus status

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

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 Topics request security utm anti-virus juniper-express-engine

clear security utm antivirus statistics

show security utm anti-virus statistics

show security utm anti-virus status

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
```

request system license update

Syntax request system license update

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Starts autoupdating license keys from the LMS server.

Options trial—Starts autoupdating trial license keys from LMS server.

Required Privilege Level maintenance

List of Sample Output request system license update on page 1028
request system license update trial on page 1028

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.
```

request system partition compact-flash

Syntax request system partition compact-flash

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 1029
request system partition compact-flash (If No) on page 1029

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 Software.

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 Topics dhcp

show system services dhcp client

List of Sample Output request system services dhcp client release ge-1/0/1 on page 1030
request system services dhcp client renew ge-1/0/1 on page 1030

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
```

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 Software.

Description The in-service software upgrade (ISSU) feature allows a chassis cluster pair to be upgraded or downgraded from supported JUNOS 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 1031

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
Inititating in-service-upgrade

node0:
--------------------------------------------------------------------------
Inititating 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.
```

request wan-acceleration login

Syntax request wan-acceleration login fpc *slot-number*

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Log in to the WXC Integrated Services Module (ISM 200) from J Series devices running JUNOS Software 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 Topics show chassis fpc

[Unresolved xref]

show wan-acceleration status

List of Sample Output request wan-acceleration login fpc 3 (permissions set) on page 1033
request wan-acceleration login fpc 3 (permissions not set) on page 1033

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 Software.

Description Upgrade access point software.

Options *name*—Upgrades 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 restart

Syntax request wlan access-point restart *name*

Release Information Command introduced in Release 10.0 of JUNOS Software.

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.
```

Chapter 25

Restart Commands

This chapter presents the **restart** operational commands available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Use the **restart** operational commands to restart software processes on the device. Operational commands are organized alphabetically.

The commands shown in this chapter are exclusive to J Series and SRX Series devices. Command options described in this chapter are marked in bold in the syntax list. For information about **restart** command options that are not explained here—commands that are shared across Juniper Networks devices—see the *JUNOS CLI User Guide*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software 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 | 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 JUNOS Release 7.4.
wan-acceleration option added in JUNOS Release 8.5.

Description Restart a JUNOS Software 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.

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 1038

Output Fields When you enter this command, you are provided feedback on the status of your request.

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

Chapter 26

Show Commands

This chapter presents the show operational commands available on J Series Services Routers and SRX Series Services Gateways running JUNOS Software. Use the show operational commands to review and verify the validity of your configurations and monitor device operation. Operational commands are organized alphabetically.

The commands shown in this chapter are exclusive to J Series and SRX Series devices. For information about show commands that are not explained here—commands that are shared across Juniper Networks devices—see the *JUNOS Interfaces Command Reference*, the *JUNOS Routing Protocols and Policies Command Reference*, and the *JUNOS System Basics and Services Command Reference*.

For information about features supported on different SRX Series and J Series devices, see the *JUNOS Software Feature Support Reference for SRX Series and J Series Devices*.

show bgp neighbor

Syntax show bgp neighbor
< *neighbor-address*>
<instance *instance* >

Release Information Command modified in Release 8.5 of JUNOS Software.

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 Topics *JUNOS Routing Protocols and Policies Command Reference*

List of Sample Output show bgp neighbor 5.5.5.2 on page 1042
show bgp neighbor instance master on page 1042

Output Fields Table 5 on page 1040 lists the output fields for the show bgp neighbor command. Output fields are listed in the approximate order in which they appear.

Table 5: 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 checkfailed, 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.

Table 5: 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.

Table 5: 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
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 chassis cluster control-plane statistics

Syntax show chassis cluster control-plane statistics

Release Information Command introduced in Release 9.3 of JUNOS Software. Output changed to support dual control ports in Release 10.0 of JUNOS Software.

Description Display information about chassis cluster control plane statistics.

Required Privilege Level view

Related Topics clear chassis cluster control-plane statistics

List of Sample Output show chassis cluster control-plane statistics on page 1044
show chassis cluster control-plane statistics (SRX5000 line devices) on page 1044

Output Fields Table 6 on page 1044 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 6: 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 (SRX5000 line 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.
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.

show chassis cluster control-plane statistics

```
user@host> show chassis cluster control-plane statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 124
        Heartbeat packets received: 125
Fabric link statistics:
    Probes sent: 124
    Probes received: 125
```

show chassis cluster control-plane statistics (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
```

show chassis cluster data-plane statistics

Syntax show chassis cluster data-plane statistics

Release Information Command introduced in Release 9.3 of JUNOS Software.

Description Display information about chassis cluster data plane statistics.

Required Privilege Level view

Related Topics clear chassis cluster data-plane statistics

List of Sample Output show chassis cluster data-plane statistics on page 1047

Output Fields Table 7 on page 1046 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 7: 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.

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 Software. Output changed to support dual control ports in Release 10.0 of JUNOS Software.

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 1048
show chassis cluster interfaces (SRX5000 line devices) on page 1048

Output Fields Table 8 on page 1048 lists the output fields for the show chassis cluster interfaces command. Output fields are listed in the approximate order in which they appear.

Table 8: 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 (SRX5000 line 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 (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:
    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 Software.

Description Display the status of all monitored IP addresses under a redundancy group.

Options none— Display the status of monitored IP addresses under 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 Topics redundancy-group

clear chassis cluster failover-count

request chassis cluster failover node

request chassis cluster failover reset

List of Sample Output show chassis cluster ip-monitoring status on page 1050
show chassis cluster ip-monitoring status redundancy-group on page 1051

Output Fields Table 9 on page 1050 lists the output fields for the show chassis cluster ip-monitoring status command. Output fields are listed in the approximate order in which they appear.

Table 9: 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.
Weight	Relative assigned value of the reachability of the monitored IP address.
Status	Current reachability state (Reachable or Unreachable) of the monitored IP address.

show chassis cluster ip-monitoring status

```
user@host> show chassis cluster ip-monitoring status
Redundancy-group      IP Address      Weight        Status
     1                1.2.3.4         20            Unreachable
     2                56.0.0.10       100           Reachable
```

show chassis cluster ip-monitoring status redundancy-group

```
user@host> show chassis cluster ip-monitoring status redundancy-group 2
Redundancy-group      IP Address      Weight        Status
      2               56.0.0.10       100           Reachable
```

show chassis cluster statistics

Syntax show chassis cluster statistics

Release Information Command modified in Release 9.0 of JUNOS Software. Output changed to support dual control ports in Release 10.0 of JUNOS Software.

Description Display information about chassis cluster services and interfaces.

Required Privilege Level view

Related Topics clear chassis cluster statistics

List of Sample Output show chassis cluster statistics on page 1053
show chassis cluster statistics (SRX5000 line devices) on page 1054
show chassis cluster statistics (SRX5000 line devices) on page 1054

Output Fields Table 10 on page 1052 lists the output fields for the show chassis cluster statistics command. Output fields are listed in the approximate order in which they appear.

Table 10: 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 (SRX5000 line only). Note that the output for the SRX5000 line 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 10: 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
    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 (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 (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
```

show chassis cluster status

Syntax show chassis cluster status
<redundancy-group *group-number* >

Release Information Command modified in Release 9.2 of JUNOS Software. Output changed to support dual control ports in Release 10.0 of JUNOS Software.

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 Topics redundancy-group

clear chassis cluster failover-count

request chassis cluster failover node

request chassis cluster failover reset

List of Sample Output show chassis cluster status on page 1057
show chassis cluster status redundancy-group 2 on page 1057
show chassis cluster status on page 1057
show chassis cluster status on page 1057

Output Fields Table 11 on page 1056 lists the output fields for the show chassis cluster status command. Output fields are listed in the approximate order in which they appear.

Table 11: 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.

Table 11: 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
Redundancy group: 1 , Failover count: 41
    node0                   101         primary        no       no
    node1                   0           unavailable    n/a      n/a
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics

JUNOS System Basics and Services Command Reference

List of Sample Output

show chassis fpc on page 1060
show chassis fpc (SRX5600 and SRX5800 devices) on page 1060
show chassis fpc detail on page 1061
show chassis fpc pic-status on page 1061
show chassis fpc pic-status (SRX5600 and SRX5800 devices) on page 1061

Output Fields

Table 12 on page 1060 lists the output fields for the show chassis fpc command. Output fields are listed in the approximate order in which they appear.

Table 12: 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 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
  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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics *JUNOS System Basics and Services Command Reference*

List of Sample Output
show chassis hardware on page 1064
show chassis hardware (SRX5600 and SRX5800 devices) on page 1064
show chassis hardware detail on page 1064
show chassis hardware detail node 1 on page 1064
show chassis hardware extensive on page 1065
show chassis hardware models (SRX5600 and SRX5800 devices) on page 1066
show chassis hardware clei-models (SRX5600 and SRX5800 devices) on page 1066

Output Fields Table 13 on page 1062 lists the output fields for the show chassis hardware command. Output fields are listed in the approximate order in which they appear.

Table 13: 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.
Part Number	Part number for the chassis component.

Table 13: show chassis hardware Output Fields *(continued)*

Field Name	Field Description
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.

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
  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
```

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 Software.

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 Topics clear esis adjacency

List of Sample Output
show esis adjacency on page 1068
show esis adjacency brief on page 1068
show esis adjacency detail on page 1068
show esis adjacency extensive on page 1068

Output Fields Table 14 on page 1067 describes the output fields for the show esis adjacency command. Output fields are listed in the approximate order in which they appear.

Table 14: 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
Advertised holdtime	Holdtime interval advertised by this neighbor.	detail extensive

Table 14: show esis adjacency Output Fields *(continued)*

Field Name	Field Description	Level of Output
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 1068.

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
```

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 Software.

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 1070
show esis interface brief on page 1070
show esis interface detail on page 1070
show esis interface extensive on page 1070

Output Fields Table 15 on page 1069 describes the output fields for the show esis interface command. Output fields are listed in the approximate order in which they appear.

Table 15: 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
End system configuration timer	Time, in seconds, for the end system to configure itself for ES-IS.	detail extensive

Table 15: show esis interface Output Fields *(continued)*

Field Name	Field Description	Level of Output
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 1070.

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 1070.

show esis statistics

Syntax show esis statistics
<instance *instance-name*>

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics clear esis statistics

List of Sample Output show esis statistics on page 1071

Output Fields Table 16 on page 1071 describes the output fields for the show esis statistics command. Output fields are listed in the approximate order in which they appear.

Table 16: 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
```

show ethernet-switching mac-learning-log

Syntax show ethernet-switching mac-learning-log

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Display the event log of learned MAC addresses.

Required Privilege Level view

Related Topics show ethernet-switching table

List of Sample Output show ethernet-switching mac-learning-log on page 1072

Output Fields Table 17 on page 1072 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 17: 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 the JUNOS Software 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
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]
```

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 Software.

Description Display 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

Related Topics show ethernet-switching mac-learning-log

List of Sample Output
show ethernet-switching table on page 1075
show ethernet-switching table brief on page 1075
show ethernet-switching table detail on page 1076
show ethernet-switching table extensive on page 1077
show ethernet-switching table interface ge-0/0/1 on page 1077

Output Fields Table 18 on page 1074 lists the output fields for the show ethernet-switching table command. Output fields are listed in the approximate order in which they appear.

Table 18: 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]
```

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
```

show gtp tunnels

Syntax show gtp tunnels <brief | summary>

Release Information Command introduced in Release 10.0 of JUNOS Software.

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 1078
show gtp tunnels summary on page 1078

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 Software.

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

Related Topics show igmp-snooping vlans

List of Sample Output
show igmp-snooping route on page 1079
show igmp-snooping route vlan v1 on page 1079

Output Fields Table 19 on page 1079 lists the output fields for the show igmp-snooping route command. Output fields are listed in the approximate order in which they appear.

Table 19: 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
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 Software.

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

Related Topics show igmp-snooping route

List of Sample Output show igmp-snooping vlans on page 1082
show igmp-snooping vlans vlan v10 on page 1082
show igmp-snooping vlans vlan v10 detail on page 1082

Output Fields Table 20 on page 1081 lists the output fields for the show igmp-snooping vlans command. Output fields are listed in the approximate order in which they appear.

Table 20: 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.

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 Software.

Description Display status information and statistics about interfaces on J Series and SRX Series devices running JUNOS Software.

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 Software Interfaces and Routing Configuration Guide*.

- 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 Topics *JUNOS Interfaces Command Reference*

List of Sample Output
show interfaces Gigabit Ethernet on page 1084
show interfaces extensive (Gigabit Ethernet) on page 1084
show interfaces terse on page 1085
show interfaces extensive (WAN Acceleration) on page 1086
show interfaces extensive (3G Wireless Modem) on page 1087

Output Fields Table 21 on page 1084 lists the output fields for the show interfaces command. Output fields are listed in the approximate order in which they appear.

Table 21: 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
```

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
   Output bytes  :                 868                   0 bps
   Input  packets:                   0                   0 pps
   Output packets:                  16                   0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runs: 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 flow-statistics

Syntax show interfaces flow-statistics <*interface-name*>

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Software Interfaces and Routing Configuration Guide*.

- 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 1090

Output Fields Table 22 on page 1089 lists the output fields for the show interfaces flow-statistics command. Output fields are listed in the approximate order in which they appear.

Table 22: 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.
Transit statistics	Number of packets and bytes transiting the physical interface.
Flow input statistics	Statistics on packets received by flow module.

Table 22: show interfaces flow-statistics Output Fields *(continued)*

Field Name	Field Description
Flow output statistics	Statistics on packets sent by flow module.
Flow error statistics	Statistics on errors in the flow module.

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 modem wireless interface

Syntax show modem wireless interface *interface-name*

Release Information Command introduced in Release 9.5 of JUNOS Software.

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 1091

Output Fields Table 23 on page 1091 lists the output fields for the show modem wireless interface command.

Table 23: 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
```

```
  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 Software.

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 1094
show modem wireless interface firmware (GSM modem) on page 1094

Output Fields Table 24 on page 1093 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 24: 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.

Table 24: 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
```

show modem wireless interface network

Syntax show modem wireless interface *interface-name* network

Release Information Command introduced in Release 9.5 of JUNOS Software.

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 1096
show modem wireless interface network (GSM modem) on page 1096

Output Fields Table 25 on page 1095 lists some of the output fields for the show modem wireless interface network command.

Table 25: 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)
Current Service Mode	One of the following: ■ High-Speed Packet Access (HSPA) ■ High-Speed Downlink Packet Access (HSDPA) ■ High-Speed Uplink Packet Access (HSUPA)

Table 25: show modem wireless interface network Output Fields *(continued)*

Field Name	Field Description
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
```

show modem wireless interface rssi

Syntax show modem wireless interface *interface-name* rssi

Release Information Command introduced in Release 9.5 of JUNOS Software.

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 1097

Output Fields Table 26 on page 1097 lists the output fields for the show modem wireless interface rssi command.

Table 26: 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
```

show network-access requests pending

Syntax show network-access requests pending
<detail>
<index *number* >

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics clear network-access requests pending

List of Sample Output show network-access requests pending on page 1099
show network-access requests pending detail on page 1099
show network-access requests pending index 1 on page 1099

Output Fields Table 27 on page 1098 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 27: 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.

Table 27: 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
```

show network-access requests statistics

Syntax show network-access requests statistics

Release Information Command modified in Release 9.1 of JUNOS Software.

Description Display authentication statistics for the configured authentication type.

Required Privilege Level view

Related Topics authentication-order

clear network-access requests statistics

Output Fields Table 28 on page 1100 lists the output fields for the network-access requests statisticscommand. Output fields are listed in the approximate order in which they appear.

Table 28: 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
```

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 Software.

Description Display the path to the node secret file for the SecurID authentication type.

Required Privilege Level view

Related Topics configuration-file

securid-server

clear network-access securid-node-secret-file

List of Sample Output show network-access securid-node-secret-file on page 1101

Output Fields Table 29 on page 1101 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 29: 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 Software.

Description Displays the status of the Power over Ethernet (PoE) controller.

Options none—Displays general parameters of the PoE software module controller.

Required Privilege Level View

Output Fields Table 30 on page 1102 lists the output fields for the show poe controller command. Output fields are listed in the approximate order in which they appear.

Table 30: 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
```

show poe interface

Syntax show poe interface <ge-fpc/pic/port>

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Displays the status of Power over Ethernet (PoE) ports.

Options none—Displays the status of all PoE ports on the SRX Series device.

ge-fpc/pic/port— (Optional) Displays the status of a specific PoE port on the SRX Series device.

Required Privilege Level View

Output Fields Table 31 on page 1103 lists the output fields for the show poe interface command. Output fields are listed in the approximate order in which they appear.

Table 31: 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
```

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 Software.

Description Displays a history of power consumption on the specified interface.

Options ge-fpc/pic/port—Displays telemetries for the specified PoE interface.

all—Displays all telemetries records for the specified PoE interface.

x—Displays the specified number of telemetries records for the specified PoE interface.

Required Privilege Level View

Output Fields Table 32 on page 1105 lists the output fields for the show poe telemetries interface command. Output fields are listed in the approximate order in which they appear.

Table 32: show poe telemetries interface Output Fields

Field name	Field Description
S1 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
```

```
5     Fri Jan 04 11:10:15 2009 6.6 W    47.2 V
```

show schedulers

Syntax show schedulers
< scheduler-name *scheduler-name* >

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics schedulers

List of Sample Output show schedulers on page 1107
show schedulers scheduler-name sch20 on page 1108

Output Fields Table 33 on page 1107 lists the output fields for the show schedulers command. Output fields are listed in the approximate order in which they appear.

Table 33: 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
```

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics h323

clear security alg h323 counters

List of Sample Output show security alg h323 counters on page 1110

Output Fields Table 34 on page 1109 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 34: 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.

Table 34: 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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics mgcp

clear security alg mgcp calls

List of Sample Output show security alg mgcp calls on page 1112
show security alg mgcp calls endpoint on page 1112

Output Fields Table 35 on page 1111 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 35: 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.

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics mgcp

clear security alg mgcp counters

List of Sample Output show security alg mgcp counters on page 1114

Output Fields Table 36 on page 1113 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 36: 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.
Number of active calls	Number of MGCP ALG active calls.
Number of active transactions	Number of active transactions.

Table 36: show security alg mgcp counters Output Fields *(continued)*

Field Name	Field Description
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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics mgcp

List of Sample Output show security alg mgcp endpoints on page 1116
show security alg mgcp endpoints d001@100.100.100.152 on page 1116

Output Fields Table 37 on page 1115 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 37: 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.
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
```

show security alg msrpc

Syntax show security alg msrpc
<object-id-map>
<portmap>

Release Information Command introduced in Release 9.0 of JUNOS Software.

Description Display Microsoft (MS) remote procedure call (RPC) Application Layer Gateway (ALG) information.

Options object-id-map—(Optional) Display information about MSRPC ID (UUID) to object ID (OID) table.

portmap—(Optional) Display information about Microsoft's implementation of the remote procedure call (MSRPC) mapping table.

Required Privilege Level view

Related Topics msrpc

"Sample Output" on page 1118

List of Sample Output
show security alg msrpc object-id-map on page 1117
show security alg msrpc portmap on page 1118

Output Fields Table 38 on page 1117 lists the output fields for the show security alg msrpc command. Output fields are listed in the approximate order in which they appear.

Table 38: show security alg msrpc Output Fields

Field Name	Field Description
UUID	MS RPC ID.
OID	MS RPC object ID.
IP	IP address of the server that maps to the MS RPC ID.
Port	Port number of the server that maps to the MS RPC ID.
Protocol	Protocol used to support the process.

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 msrpc portmap

```
user@host> show security alg msrpc portmap
    IP                Port    Protocol   UUID
    172.27.81.162     36100   TCP        1544f5e0-613c-11d1-93df-00c04fd7bd09
    172.27.81.162     516     TCP        f5cc5a18-4264-101a-8c59-08002b2f8426
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sccp

clear security alg sccp calls

List of Sample Output show security alg sccp calls on page 1120
show security alg sccp calls detail on page 1120

Output Fields Table 39 on page 1119 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 39: 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.

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sccp

clear security alg sccp counters

List of Sample Output show security alg sccp counters on page 1122

Output Fields Table 40 on page 1121 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 40: 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.
Packets dropped	Number of packets dropped by the SCCP ALG.
Decode errors	Number of decoding errors.

Table 40: show security alg sccp counters Output Fields *(continued)*

Field Name	Field Description
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

clear security alg sip calls

List of Sample Output show security alg sip calls on page 1124
show security alg sip calls detail on page 1124
show security alg sip calls node all on page 1124

Output Fields Table 41 on page 1123 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 41: show security alg sip calls Output Fields

Field Name	Field Description
UAS callid	Call Identifier for the SIP ALG user agent server.
Local Tag	Local tag for the SIP ALG user agent server.
Remote Tag	Remote tag 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: 2 (# of call legs 4)
   Call leg1: zone 3
      UAS callid:000ed748-55330007-04c3379d-0aab7e18@2.2.3.2 (pending tsx 1)
      Local tag
      Remote tag: 000ed748553300e264b0a951-5caa0a95
      State: STATE_DISCONNECTED
   Call leg2: zone 2
      UAC callid:000ed748-55330007-04c3379d-0aab7e18@2.2.3.2 (pending tsx 1)
      Local tag: 000ed748553300e264b0a951-5caa0a95
      Remote tag
      State: STATE_DISCONNECTED
   Call leg1: zone 3
      UAS callid:000ed748-55330007-04c3379d-0aab7e18@2.2.3.2 (pending tsx 1)
      Local tag:  000f90542e7e64cd724880f5-65db2f99
      Remote tag: 000ed748553300e264b0a951-5caa0a95
      State: STATE_ESTABLISHED
   Call leg2: zone 2
      UAC callid:000ed748-55330007-04c3379d-0aab7e18@2.2.3.2 (pending tsx 1)
      Local tag:  000ed748553300e264b0a951-5caa0a95
      Remote tag: 000f90542e7e64cd724880f5-65db2f99
      State: STATE_ESTABLISHED
```

show security alg sip calls detail

```
user@host> show security alg sip calls detail
Total number of calls: 1
       Call ID    : 000ed748-5533005e-11d97de9-77759865@10.10.10.254
       Local tag  : 000f90542e7e005c7807c3a0-0647d41e
       Remote tag : 000ed748553300724648b313-2ccd0d9a
       State      : STATE_ESTABLISHED               RM Group:2048
                    Local Info              Remote Info            RM Info
                    ----------              -----------            -------
       Call leg 1:  IP             Port     IP             Port     RSC id

         Host       10.10.10.10    5060     10.10.10.10    5060
         Contact    10.10.10.100   5060     10.10.10.254   1025     8191
         Contact maddr-                       -
         SDP:c      10.10.10.100             10.10.10.254
         SDP:m      10.10.10.100   18902    10.10.10.254   64518 8192 ,8185
       Call leg 2:
         Host       10.10.10.10    5060     10.10.10.10    5060
         Contact    10.10.10.254   1025     10.10.10.100   5060     8188
         Contact maddr-                       -
         SDP:c      10.10.10.254             10.10.10.100
         SDP:m      10.10.10.254   64518    10.10.10.100   18902 8186 ,8187
```

show security alg sip calls node all

```
user@host> show security alg sip calls node all
node0:
--------------------------------------------------------------------------
Total number of calls: 1
Call leg 1 Zone : 6
  UAS call ID: 00078513-12490005-2ca7b914-2b5ea3b3@26.0.29.236 (pending
transactions 0)
  Local tag  : 00036bb9112700267368b9d7-423830f3
  Remote tag : 000785131249002902c91c61-0a9627ad
  State      : STATE_ESTABLISHED
Call leg 2 Zone : 8
  UAC call ID: 00078513-12490005-2ca7b914-2b5ea3b3@11.0.100.196:1050 (pending
transactions 0)
  Local tag  : 000785131249002902c91c61-0a9627ad
  Remote tag : 00036bb9112700267368b9d7-423830f3
```

```
  State      : STATE_ESTABLISHED

node1:
--------------------------------------------------------------------------
Total number of calls: 1
Call leg 1 Zone : 6
  UAS call ID: 00078513-12490005-2ca7b914-2b5ea3b3@26.0.29.236 (pending
transactions 0)
  Local tag  : 00036bb9112700267368b9d7-423830f3
  Remote tag : 000785131249002902c91c61-0a9627ad
  State      : STATE_ESTABLISHED
Call leg 2 Zone : 8
  UAC call ID: 00078513-12490005-2ca7b914-2b5ea3b3@11.0.100.196:1050 (pending
transactions 0)
  Local tag  : 000785131249002902c91c61-0a9627ad
  Remote tag : 00036bb9112700267368b9d7-423830f3
  State      : STATE_ESTABLISHED
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

clear security alg sip counters

List of Sample Output show security alg sip counters on page 1128

Output Fields Table 42 on page 1126 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 42: 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.
RR header exceeded max	Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit.

Table 42: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
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.
Total Pkt dropped on error	Number of SIP ALG total packets dropped while transmission and retransmission of messages.
Transaction error	Number of SIP ALG transaction errors.

Table 42: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
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     0    0     0     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     0    0     0     0    0     0     0
               0    0     0     0    0     0     0
       BYE     0    0     0     0    0     0     0
               0    0     0     0    0     0     0
  REGISTER     0    0     0     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
               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                        :15
Total Pkt dropped on error          :0
Transaction 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
Invite Dropped due to call limit    :0
SIP msg not processed by stack      :0
SIP msg not processed by alg        :0
SIP unknown method dropped          :0
Decoding error                      :0
Request for disconnected call       :0
Request out of state                :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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

List of Sample Output show security alg sip rate on page 1130

Output Fields Table 43 on page 1130 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 43: 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
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics sip

List of Sample Output show security alg sip transactions on page 1131

Output Fields Table 44 on page 1131 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 44: 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
```

show security alg status

Syntax show security alg status

Release Information Command modified in Release 9.5 of JUNOS Software

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 Software Security Configuration Guide*.

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
- 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
```

show security alg sunrpc portmap

Syntax show security alg sunrpc portmap

Release Information Command introduced in Release 9.0 of JUNOS Software.

Description Display Sun Microsystems remote procedure call (RPC) ALG information.

Options portmap—Display Sun Microsystem remote procedure call (SUNRPC) mapping table information.

Required Privilege Level view

Related Topics sunrpc

clear security alg sunrpc portmap

List of Sample Output show security alg sunrpc portmap on page 1134

Output Fields Table 45 on page 1134 lists the output fields for the show security alg sunrpc portmap command. Output fields are listed in the approximate order in which they appear.

Table 45: show security alg sunrpc portmap Output Fields

Field Name	Field Description
IP	IP address of the server that maps to the program.
Port	Port number of the server that maps to the program.
Protocol	Protocol used to support the process.
Program	Program ID number.

show security alg sunrpc portmap

```
user@host> show security alg sunrpc portmap
IP                Port    Protocol   Program
10.209.17.127     32835   TCP        100005
10.209.17.127     2049    UDP        100003
10.209.17.127     111     UDP        100000
10.209.17.127     111     TCP        100000
```

show security datapath-debug capture

Syntax show security datapath—debug capture

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description Displays details of the data path-debugging capture file.

Required Privilege Level view

List of Sample Output show security datapath—debug capture on page 1135

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
```

show security datapath-debug capture

Syntax show security datapath-debug capture

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description Displays details of the data path debugging capture file.

Required Privilege Level view

Related Topics show security datapath-debug counter

List of Sample Output show security datapath—debug capture on page 1136

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
```

show security datapath-debug counter

Syntax show security datapath-debug counter

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description Displays details of the data path debugging counter.

Required Privilege Level view

Related Topics show security datapath-debug capture

List of Sample Output show security datapath-debug counter on page 1137

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
```

show security dynamic-vpn client version

Syntax show security dynamic-vpn client version

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description This command displays the client software version.

Required Privilege Level view

Output Fields user@host> show security dynamic-vpn client version

Sample Output

```
Juniper Access Manager version: 1.1.0.4165
```

show security dynamic-vpn users

Syntax show security dynamic-vpn users

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description This command shows the relevant user information such as username, source IP, IKE ID, name of IPsec VPN, name of IKE gateway, and number of connections currently active.

Required Privilege Level view

Output Fields user@host> show security dynamic-vpn users

Sample Output

```
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
```

show security dynamic-vpn users terse

Syntax show security dynamic-vpn users terse

Release Information This command was introduced in Release 10.0 of JUNOS Software.

Description This command displays all relevant user information such as username, source IP, IKE ID, name of IPsec VPN, name of IKE gateway, and the number of connections currently active in a table.

Required Privilege Level view

Output Fields user@host> show security dynamic-vpn users terse

Sample Output

```
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication history

List of Sample Output show security firewall-authentication history on page 1142
show security firewall-authentication history node all on page 1142

Output Fields Table 46 on page 1141 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 46: 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.
Status	Authentication status success or failure.

Table 46: show security firewall-authentication history Output Fields *(continued)*

Field Name	Field Description
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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication history address

List of Sample Output show security firewall-authentication history address 4.4.4.2 on page 1144
show security firewall-authentication history address 100.0.0.1 node local on page 1144

Output Fields Table 47 on page 1143 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 47: 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.
Access start time	Time when user authenticated.

Table 47: show security firewall-authentication history address Output Fields *(continued)*

Field Name	Field Description
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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication history identifier

List of Sample Output show security firewall-authentication history identifier 1 on page 1147
show security firewall-authentication identifier 1 node primary on page 1147

Output Fields Table 48 on page 1146 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 48: 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.
Access start date	Date when user authenticated.

Table 48: show security firewall-authentication history identifier 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 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
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication users

List of Sample Output show security firewall-authentication users on page 1149
show security firewall-authentication users node 0 on page 1149
show security firewall-authentication users node all on page 1149

Output Fields Table 49 on page 1148 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 49: 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.
Age	Idle timeout for the user.

Table 49: show security firewall-authentication users Output Fields *(continued)*

Field Name	Field Description
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication users address

List of Sample Output show security firewall-authentication users address 211.0.0.6 on page 1151
show security firewall-authentication users address 100.0.0.1 node local on page 1151

Output Fields Table 50 on page 1150 lists the output fields for the show security firewall-authentication users addresscommand. Output fields are listed in the approximate order in which they appear.

Table 50: 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.
Source zone	User traffic received from the zone.

Table 50: show security firewall-authentication users address Output Fields *(continued)*

Field Name	Field Description
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics firewall-authentication (Security)

clear security firewall-authentication users identifier

List of Sample Output show security firewall-authentication users identifier 3 on page 1153
show security firewall-authentication users identifier 3 node primary on page 1153

Output Fields Table 51 on page 1152 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 51: 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.
Access time remaining	Duration for which the connection exists.

Table 51: show security firewall-authentication users identifier Output Fields *(continued)*

Field Name	Field Description
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 gate

Syntax show security flow gate
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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 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 Topics flow

List of Sample Output show security flow gate on page 1155
show security flow gate node 0 on page 1156

Output Fields Table 52 on page 1154 lists the output fields for the show security flow gate command. Output fields are listed in the approximate order in which they appear.

Table 52: 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.

Table 52: show security flow gate 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.

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 node 0

```
user@host> show security flow gate node 0
node0:
--------------------------------------------------------------------------

Hole: 0.0.0.0-0.0.0.0/0-0->11.0.30.21-11.0.30.21/24923-24923
  Translated: 0.0.0.0/0->11.0.30.21/24923
  Protocol: udp
  Application: none/0
  Age: 89 seconds
  Flags: 0xe001
  Zone: trust
  Reference count: 1
  Resource: 5-1024-8192
Hole: 0.0.0.0-0.0.0.0/0-0->11.0.54.20-11.0.54.20/5060-5060
  Translated: 0.0.0.0/0->11.0.54.20/5060
  Protocol: udp
  Application: junos-sip/63
  Age: 65535 seconds
  Flags: 0xe200
  Zone: trust
  Reference count: 1
  Resource: 5-1024-8188

Hole: 0.0.0.0-0.0.0.0/0-0->11.0.100.196-11.0.100.196/64511-64511
  Translated: 0.0.0.0/0->26.0.29.236/25897
  Protocol: udp
  Application: none/0
  Age: 88 seconds
  Flags: 0xe001
  Zone: dmz
  Reference count: 1
  Resource: 5-1024-8187

Hole: 0.0.0.0-0.0.0.0/0-0->11.0.100.196-11.0.100.196/64510-64510
  Translated: 0.0.0.0/0->26.0.29.236/25896
  Protocol: udp
  Application: none/0
  Age: 88 seconds
  Flags: 0xe001
  Zone: dmz
  Reference count: 1
  Resource: 5-1024-8190

Hole: 0.0.0.0-0.0.0.0/0-0->11.0.100.196-11.0.100.196/1024-1024
  Translated: 11.0.54.20/41968->26.0.29.236/5060
  Protocol: udp
  Application: junos-sip/63
  Age: 65535 seconds
  Flags: 0xe200
  Zone: dmz
  Reference count: 1
  Resource: 5-1024-8186
```

show security flow session

Syntax show security flow session
node (*node-id* | all | local | primary)

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about all currently active security sessions on the device.

Options none—Display information about all active sessions.

node—(Optional) For chassis cluster configurations, display all active sessions 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 Topics flow

clear security flow session all

List of Sample Output show security flow session on page 1157
show security flow session node all on page 1158

Output Fields Table 53 on page 1157 lists the output fields for the show security flow session command. Output fields are listed in the approximate order in which they appear.

Table 53: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session

```
user@host> show security flow session
Session ID: 2102, Policy name: self-traffic-policy/1, Timeout: 272
  In: 172.24.68.74/3428 --> 10.157.84.52/23;tcp, If: ge-0/0/0.0
```

```
  Out: 10.157.84.52/23 --> 172.24.68.74/3428;tcp, If: .local..0
Session ID: 2111, Policy name: self-traffic-policy/1, Timeout: 1800
  In: 172.24.68.97/3175 --> 10.157.84.52/23;tcp, If: ge-0/0/0.0
  Out: 10.157.84.52/23 --> 172.24.68.97/3175;tcp, If: .local..0
Session ID: 2112, Policy name: self-traffic-policy/1, Timeout: 1781
  In: 172.24.68.97/3176 --> 10.157.84.52/23;tcp, If: ge-0/0/0.0
  Out: 10.157.84.52/23 --> 172.24.68.97/3176;tcp, If: .local..0
3 sessions displayed
```

show security flow session node all

```
user@host> show security flow session node all
node0:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Active, Timeout: 60
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
Session ID: 2, Policy name: sfw2/5, State: Active, Timeout: 60
  In: 1.1.2.2/2000 --> 11.11.2.2/40000;udp, If: reth0.2
  Out: 11.11.2.2/40000 --> 1.1.2.2/2000;udp, If: reth1.2
Session ID: 3, Policy name: sfw3/6, State: Active, Timeout: 60
  In: 1.1.3.2/2000 --> 11.11.3.2/40000;udp, If: reth0.3
  Out: 11.11.3.2/40000 --> 1.1.3.2/2000;udp, If: reth1.3
Session ID: 4, Policy name: sfw4/7, State: Active, Timeout: 60
  In: 1.1.4.2/2000 --> 11.11.4.2/40000;udp, If: reth0.4
  Out: 11.11.4.2/40000 --> 1.1.4.2/2000;udp, If: reth1.4
4 sessions displayed
node1:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Backup, Timeout: 482
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
Session ID: 2, Policy name: sfw2/5, State: Backup, Timeout: 476
  In: 1.1.2.2/2000 --> 11.11.2.2/40000;udp, If: reth0.2
  Out: 11.11.2.2/40000 --> 1.1.2.2/2000;udp, If: reth1.2
Session ID: 3, Policy name: sfw3/6, State: Backup, Timeout: 480
  In: 1.1.3.2/2000 --> 11.11.3.2/40000;udp, If: reth0.3
  Out: 11.11.3.2/40000 --> 1.1.3.2/2000;udp, If: reth1.3
Session ID: 4, Policy name: sfw4/7, State: Backup, Timeout: 482
  In: 1.1.4.2/2000 --> 11.11.4.2/40000;udp, If: reth0.4
  Out: 11.11.4.2/40000 --> 1.1.4.2/2000;udp, If: reth1.4
4 sessions displayed
```

show security flow session application

Syntax show security flow session application
application-name
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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

- dnsDomain Name System
- ftpFile Transfer Protocol
- ignoreIgnore application type
- mgcp-caMedia Gateway Control Protocol with Call Agent
- mgcp-uaMGCP with User Agent
- pptpPoint-to-Point Tunneling Protocol
- q931ISDN connection control protocol
- rasRAS
- realaudioRealAudio
- rshUNIX remote shell services
- rtspReal-Time Streaming Protocol
- sccpSkinny Client Control Protocol
- sipSession Initiation Protocol
- sqlnet-v2Oracle SQLNET
- talkTALK program
- tftpTrivial File Transfer Protocol

node—(Optional) For chassis cluster configurations, display sessions for the specified application type or application set 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 Topics clear security flow session application

List of Sample Output

show security flow session application ftp on page 1160
show security flow session application sip node primary on page 1160

Output Fields

Table 54 on page 1160 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 54: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session application ftp

```
user@host> show security flow session application ftp
Session ID: 33, Policy name: default-policy/2, Timeout: 1492
  In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp, If: t1-1/0/0.0
  Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp, If: ge-0/0/1.0
```

show security flow session application sip node primary

```
user@host> show security flow session application sip node primary
node0:
--------------------------------------------------------------------------

Session ID: 246, Policy name: trust_to_dmz/4, State: Active, Timeout: 6
  In: 26.0.29.236/50039 --> 11.0.54.20/5060;udp, If: reth0.0
  Out: 11.0.54.20/5060 --> 11.0.100.196/1047;udp, If: reth2.0

Session ID: 253, Policy name: trust_to_dmz/4, State: Active, Timeout: 4
  In: 26.0.29.236/50055 --> 11.0.54.20/5060;udp, If: reth0.0
  Out: 11.0.54.20/5060 --> 11.0.100.196/1048;udp, If: reth2.0
Session ID: 254, Policy name: trust_to_dmz/4, State: Active, Timeout: 64
Resource information : SIP ALG, 1024, 8186
  In: 11.0.54.20/41968 --> 11.0.100.196/1024;udp, If: reth2.0
  Out: 26.0.29.236/5060 --> 11.0.54.20/41968;udp, If: reth0.0

3 sessions displayed
```

show security flow session destination-port

Syntax show security flow session destination-port
destination-port-number
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about each session that uses the specified destination port.

Options *destination-port-number* —Number of the destination port about which to display sessions information.

Range: 1 through 65535

node—(Optional) For chassis cluster configurations, display sessions for the specified destination port 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 Topics clear security flow session destination-port

List of Sample Output show security flow session destination-port 21 on page 1162
show security flow session destination-port 40000 node local on page 1162

Output Fields Table 55 on page 1161 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 55: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session destination-port 21

```
user@host> show security flow session destination-port 21
Session ID: 33, Policy name: default-policy/2, Timeout: 1492
  In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp, If: t1-1/0/0.0
  Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp, If: ge-0/0/1.0
```

show security flow session destination-port 40000 node local

```
user@host> show security flow session destination-port 40000 node local
node0:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Active, Timeout: 60
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
Session ID: 2, Policy name: sfw2/5, State: Active, Timeout: 60
  In: 1.1.2.2/2000 --> 11.11.2.2/40000;udp, If: reth0.2
  Out: 11.11.2.2/40000 --> 1.1.2.2/2000;udp, If: reth1.2
Session ID: 3, Policy name: sfw3/6, State: Active, Timeout: 60
  In: 1.1.3.2/2000 --> 11.11.3.2/40000;udp, If: reth0.3
  Out: 11.11.3.2/40000 --> 1.1.3.2/2000;udp, If: reth1.3
Session ID: 4, Policy name: sfw4/7, State: Active, Timeout: 60
  In: 1.1.4.2/2000 --> 11.11.4.2/40000;udp, If: reth0.4
  Out: 11.11.4.2/40000 --> 1.1.4.2/2000;udp, If: reth1.4
4 sessions displayed
```

show security flow session destination-prefix

Syntax show security flow session destination-prefix
destination-IP-prefix
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about each session that matches the specified IPv4 destination prefix.

Options *destination-IP-prefix* —Destination IPv4 prefix or address about which to display session information.

node—(Optional) For chassis cluster configurations, display sessions that match the specified destination prefix 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 Topics clear security flow session destination-prefix

List of Sample Output show security flow session destination-prefix 192.168/16 on page 1164
show security flow session destination-prefix 11.11.1.2 node primary on page 1164

Output Fields Table 56 on page 1163 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 56: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session destination-prefix 192.168/16

```
user@host> show security flow session destination-prefix 192.168/16
Session ID: 33, Policy name: default-policy/2, Timeout: 1492
  In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp, If: t1-1/0/0.0
  Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp, If: ge-0/0/1.0
```

show security flow session destination-prefix 11.11.1.2 node primary

```
user@host> show security flow session destination-prefix 11.11.1.2 node primary
node0:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Active, Timeout: 60
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
1 sessions displayed
```

show security flow session interface

Syntax show security flow session interface
interface-name
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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 router for which to display sessions information.

node—(Optional) For chassis cluster configurations, display sessions that use the specified interface 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 Topics clear security flow session interface

List of Sample Output show security flow session interface Gigabit Ethernet on page 1166
show security flow session interface reth0.1 node local on page 1166

Output Fields Table 57 on page 1165 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 57: 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 address, application protocol, and interface).
Out	Reverse flow (source and destination IP address, application protocol, and interface).

show security flow session interface Gigabit Ethernet

```
user@host> show security flow session interface ge-0/0/0.0
Session ID: 1658, Policy name: self-traffic-policy/1, Timeout: 1800
  In: 172.23.9.135/3998 --> 10.157.84.52/23;tcp, If: ge-0/0/0.0
  Out: 10.157.84.52/23 --> 172.23.9.135/3998;tcp, If: .local..0
1 sessions displayed
```

show security flow session interface reth0.1 node local

```
user@host> show security flow session interface reth0.1 node local
node0:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Active, Timeout: 60
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
1 sessions displayed
```

show security flow session protocol

Syntax show security flow session protocol (*protocol-name* | *protocol-number*)
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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

node—(Optional) For chassis cluster configurations, display sessions that use the specified protocol 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 Topics clear security flow session protocol

List of Sample Output

show security flow session protocol udp on page 1168
show security flow session protocol tcp on page 1168
show security flow session protocol udp node primary on page 1168

Output Fields

Table 58 on page 1168 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 58: 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, and interface).
Out	Reverse flow (Source and destination IP addresses, application protocol, and interface).

show security flow session protocol udp

```
user@host> show security flow session protocol udp
Session ID: 1, Policy name: self-traffic-policy/1, Timeout: 57
In: 0.0.0.0/68 --> 255.255.255.255/67;udp, If: ge-0/0/0.0
Out: 255.255.255.255/67 --> 0.0.0.0/68;udp, If: .local..0
```

show security flow session protocol tcp

```
user@host> show security flow session protocol tcp
Session ID: 4135, Policy name: N/A, Timeout: 1799
In: 10.0.0.96/1026 --> 10.0.0.1/5000;tcp, If: pc-5/0/0.16383
Out: 10.0.0.1/5000 --> 10.0.0.96/1026;tcp, If: .local..0
Session ID: 6301, Policy name: wx2ut, Timeout: 1726
In: 2.2.2.1/1865 --> 90.0.0.5/3578;tcp, If: wx-5/0/0.0
Out: 90.0.0.5/3578 --> 2.2.2.1/1865;tcp, If: e1-2/0/0.0
Session ID: 6307, Policy name: ut2wx, Timeout: 1726
In: 90.0.0.5/3331 --> 2.2.2.1/3578;tcp, If: e1-2/0/0.0
Out: 2.2.2.1/3578 --> 90.0.0.5/3331;tcp, If: wx-5/0/0.0
Session ID: 6329, Policy name: ut2wx, Timeout: 494
In: 90.0.0.6/3336 --> 2.2.2.3/3578;tcp, If: e1-2/0/1.0
Out: 2.2.2.3/3578 --> 90.0.0.6/3336;tcp, If: wx-5/0/0.0
Session ID: 6348, Policy name: ut2t_red, Timeout: 1605
In: 90.0.0.1/3972 --> 20.0.0.1/21;tcp, If: e1-2/0/0.0
Out: 20.0.0.1/21 --> 90.0.0.1/3972;tcp, If: ge-0/0/1.0
Session ID: 6355, Policy name: t2ut_red, Timeout: 1726
In: 20.0.0.1/1104 --> 90.0.0.1/21;tcp, If: ge-0/0/1.0
Out: 90.0.0.1/21 --> 20.0.0.1/1104;tcp, If: e1-2/0/0.0
6 sessions displayed
```

show security flow session protocol udp node primary

```
user@host> show security flow session protocol udp node primary
node0:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Active, Timeout: 60
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
Session ID: 2, Policy name: sfw2/5, State: Active, Timeout: 60
```

```
  In: 1.1.2.2/2000 --> 11.11.2.2/40000;udp, If: reth0.2
  Out: 11.11.2.2/40000 --> 1.1.2.2/2000;udp, If: reth1.2
Session ID: 3, Policy name: sfw3/6, State: Active, Timeout: 60
  In: 1.1.3.2/2000 --> 11.11.3.2/40000;udp, If: reth0.3
  Out: 11.11.3.2/40000 --> 1.1.3.2/2000;udp, If: reth1.3
Session ID: 4, Policy name: sfw4/7, State: Active, Timeout: 60
  In: 1.1.4.2/2000 --> 11.11.4.2/40000;udp, If: reth0.4
  Out: 11.11.4.2/40000 --> 1.1.4.2/2000;udp, If: reth1.4
4 sessions displayed
```

show security flow session resource-manager

Syntax show security flow session resource-manager
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about sessions created by the resource manager.

Options none—Display all resource manager sessions.

node—(Optional) For chassis cluster configurations, display resource manager sessions 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 Topics clear security flow session resource-manager

List of Sample Output show security flow session resource-manager on page 1171
show security flow session resource-manager node 0 on page 1171
show security flow session resource-manager node 1 on page 1171

Output Fields Table 59 on page 1170 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 59: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session resource-manager

```
user@host> show security flow session resource-manager
Session ID: 2218, Policy name: foo/4, Timeout: 60
Resource information : MGCP ALG, 2047, 8188
  In: 12.0.102.26/28072 --> 11.0.101.236/23252;udp, If: ge-0/0/2.0
  Out: 11.0.101.236/23252 --> 12.0.102.26/28072;udp, If: ge-0/0/1.0
```

show security flow session resource-manager node 0

```
user@host> show security flow session resource-manager node 0
node0:
--------------------------------------------------------------------------

Session ID: 254, Policy name: trust_to_dmz/4, State: Active, Timeout: 36
Resource information : SIP ALG, 1024, 8186
  In: 11.0.54.20/41968 --> 11.0.100.196/1024;udp, If: reth2.0
  Out: 26.0.29.236/5060 --> 11.0.54.20/41968;udp, If: reth0.0

Session ID: 255, Policy name: trust_to_dmz/4, State: Active, Timeout: 120
Resource information : SIP ALG, 1024, 8191
  In: 26.0.29.236/25896 --> 11.0.30.21/24922;udp, If: reth0.0
  Out: 11.0.30.21/24922 --> 11.0.100.196/64510;udp, If: reth2.0

2 sessions displayed
```

show security flow session resource-manager node 1

```
user@host> show security flow session resource-manager node 1
node1:
--------------------------------------------------------------------------

Session ID: 250, Policy name: trust_to_dmz/4, State: Backup, Timeout: 880
Resource information : SIP ALG, 1022, 8192
  In: 11.0.54.20/41968 --> 11.0.100.196/1024;udp, If: reth2.0
  Out: 26.0.29.236/5060 --> 11.0.54.20/41968;udp, If: reth0.0

Session ID: 251, Policy name: trust_to_dmz/4, State: Backup, Timeout: 894
Resource information : SIP ALG, 1022, 8180
  In: 26.0.29.236/25896 --> 11.0.30.21/24922;udp, If: reth0.0
  Out: 11.0.30.21/24922 --> 11.0.100.196/64510;udp, If: reth2.0

2 sessions displayed
```

show security flow session session-identifier

Syntax show security flow session session-identifier
session-identifier
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display detailed information about the session with this identifier.

Options *session-identifier* —Identifier of the session about which to display information.

node—(Optional) For chassis cluster configurations, display session information about the sessions with this identifier 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 Topics clear security flow session session-identifier

List of Sample Output show security flow session session-identifier 36 on page 1173
show security flow session session-identifier 2218 on page 1174
show security flow session session-identifier 33 on page 1174
show security flow session session-identifier 1 node primary on page 1174

Output Fields Table 60 on page 1172 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 60: 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.

Table 60: show security flow session session-identifier Output Fields *(continued)*

Field Name	Field Description
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	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
    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 session-identifier 1 node primary

```
user@host> show security flow session session-identifier 1 node primary
node0:
--------------------------------------------------------------------------
Session ID: 1, Status: Normal, State: Active
Flag: 0x40
Virtual system: root, Policy name: sfw1/4
Maximum timeout: 60, Current timeout: 60
Start time: 472, Duration: 142
   In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp,
    Interface: reth0.1,
    Session token: 0xa, Flag: 0x1
    Route: 0x1bfb01, Gateway: 1.1.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
   Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp,
    Interface: reth1.1,
    Session token: 0x12, Flag: 0x0
    Route: 0x1b9b01, Gateway: 11.11.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
```

```
    FIN state: 0,
1 sessions displayed
```

show security flow session source-port

Syntax show security flow session source-port
source-port-number
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

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.

node—(Optional) For chassis cluster configurations, display sessions for the specified source port 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 Topics clear security flow session source-port

List of Sample Output show security flow session source-port 2851 on page 1177
show security flow session source-port 2000 node 1 on page 1177

Output Fields Table 61 on page 1176 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 61: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session source-port 2851

```
user@host> show security flow session source-port 2851
Session ID: 33, Policy name: default-policy/2, Timeout: 1492
  In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp, If: t1-1/0/0.0
  Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp, If: ge-0/0/1.0
```

show security flow session source-port 2000 node 1

```
user@host> show security flow session source-port 2000 node 1
node1:
--------------------------------------------------------------------------
Session ID: 1, Policy name: sfw1/4, State: Backup, Timeout: 322
  In: 1.1.1.2/2000 --> 11.11.1.2/40000;udp, If: reth0.1
  Out: 11.11.1.2/40000 --> 1.1.1.2/2000;udp, If: reth1.1
Session ID: 2, Policy name: sfw2/5, State: Backup, Timeout: 316
  In: 1.1.2.2/2000 --> 11.11.2.2/40000;udp, If: reth0.2
  Out: 11.11.2.2/40000 --> 1.1.2.2/2000;udp, If: reth1.2
Session ID: 3, Policy name: sfw3/6, State: Backup, Timeout: 320
  In: 1.1.3.2/2000 --> 11.11.3.2/40000;udp, If: reth0.3
  Out: 11.11.3.2/40000 --> 1.1.3.2/2000;udp, If: reth1.3
Session ID: 4, Policy name: sfw4/7, State: Backup, Timeout: 322
  In: 1.1.4.2/2000 --> 11.11.4.2/40000;udp, If: reth0.4
  Out: 11.11.4.2/40000 --> 1.1.4.2/2000;udp, If: reth1.4
4 sessions displayed
```

show security flow session source-prefix

Syntax show security flow session source-prefix
source-prefix-number
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about each session that uses the specified source prefix.

Options *source-prefix-number* —Source IPv4 prefix or address about which to display sessions information.

node—(Optional) For chassis cluster configurations, display sessions for the specified source prefix 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 Topics clear security flow session source-prefix

List of Sample Output show security flow session source-prefix 10/8 on page 1179

Output Fields Table 62 on page 1178 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 62: 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, and interface).
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).

show security flow session source-prefix 10/8

```
user@host> show security flow session source-prefix 10/8
Session ID: 36, Policy name: foo/4, Timeout: 1547
  In: 10.10.10.1/4923 --> 3.3.3.2/23;tcp, If: t1-1/0/0.0
  Out: 3.3.3.2/23 --> 10.10.10.1/4923;tcp, If: .local..0
1 sessions displayed
```

show security flow session summary

Syntax show security flow session summary
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display summary information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.

Options none—Display details summary of all sessions.

node—(Optional) For chassis cluster configurations, display a summary of sessions 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 Topics clear security flow session all

List of Sample Output
show security flow session summary on page 1181
show security flow session summary (SRX Series devices) on page 1181
show security flow session summary node all on page 1181
show security flow session summary member primary on page 1181

Output Fields Table 63 on page 1180 lists the output fields for the show security flow session summary command. Output fields are listed in the approximate order in which they appear.

Table 63: show security flow session summary Output Fields

Field Name	Field Description
Unicast-sessions	Total number of active unicast sessions.
Multicast-sessions	Total number of active multicast sessions.
Failed-sessions	Total number of failed sessions.
Active-sessions	Total number of active sessions.
Maximum-sessions	Maximum number of supported sessions.

show security flow session summary

```
user@host> show security flow session summary
Session summary:
  Unicast-sessions: 1
  Multicast-sessions: 0
  Failed-sessions: 0
  Active-sessions: 1
  Maximum-sessions: 256000
```

show security flow session summary (SRX Series devices)

```
user@host> show security flow session summary
Session summary:
  Unicast-sessions: 0
  Multicast-sessions: 0
  Failed-sessions: 0
  Sessions-in-use: 0
  Maximum-sessions: 131072
  Unicast-sessions: 0
  Multicast-sessions: 0
  Failed-sessions: 0
  Sessions-in-use: 0
  Maximum-sessions: 524288
```

show security flow session summary node all

```
user@host> show security flow session summary node all
node0:
--------------------------------------------------------------------------
Session summary:
  Unicast-sessions: 4
  Multicast-sessions: 0
  Failed-sessions: 0
  Sessions-in-use: 4
  Maximum-sessions: 262144
node1:
--------------------------------------------------------------------------
Session summary:
  Unicast-sessions: 4
  Multicast-sessions: 0
  Failed-sessions: 0
  Sessions-in-use: 4
  Maximum-sessions: 262144
```

show security flow session summary member primary

```
user@host> show security flow session summary member primary
Session summary:
  Unicast-sessions: 1
  Multicast-sessions: 0
  Failed-sessions: 0
  Active-sessions: 1
  Maximum-sessions: 10000
```

show security flow session tunnel

Syntax show security flow session tunnel
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Release 8.5 of JUNOS Software; node options added in Release 9.0 of JUNOS Software.

Description Display information about all tunnel sessions.

Options none—Display all tunnel sessions.

node—(Optional) For chassis cluster configurations, display tunnel sessions 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 Topics no-syn-check-in-tunnel

clear security flow session all

List of Sample Output show security flow session tunnel on page 1182

Output Fields Table 64 on page 1182 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 64: 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, and interface).

show security flow session tunnel

```
user@host> show security flow session tunnel
Session ID: 9003, Policy name: N/A, Timeout: N/A
  In: 2.2.2.2/0 --> 2.2.2.1/0;esp, If: fe-4/0/0.0
Session ID: 9004, Policy name: N/A, Timeout: N/A
  In: 2.2.2.2/48468 --> 2.2.2.1/48442;esp, If: fe-4/0/0.0
```

```
Session ID: 9005, Policy name: N/A, Timeout: N/A
  In: 10.157.89.106/2048 --> 10.157.89.210/2048;gre, If: ge-0/0/1.0
```

show security idp active-policy

Syntax show security idp active-policy

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 Topics request security idp security-package download

request security idp security-package install

List of Sample Output show security idp active-policy on page 1184

Output Fields Table 65 on page 1184 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 65: 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
```

show security idp application-ddos application

Syntax show security idp application-ddos application

Release Information Command introduced in Release 10.0 of JUNOS Software.

Description Display basic statistics for the servers being protected by the IDP application–evel DDoS feature.

Options *application–name* —Display information on a specific AppDDos 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

Related Topics

List of Sample Output show security idp application-ddos application on page 1185
show security idp application-ddos application detail on page 1186

Output Fields Table 66 on page 1185 lists the output fields for the show security idp application-ddos application command.

Table 66: 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 AppDDos 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

...
```

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/sec
Context: 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/sec
Context: 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

...
```

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 Software.

Description Display application ID from default port/protocol binding or from the application system cache.

Required Privilege Level view

Related Topics application-system-cache

clear security idp application-identification application-system-cache

List of Sample Output show security idp application-identification application-system-cache on page 1187

Output Fields Table 67 on page 1187 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 67: show security idp application-identification application-system-cache Output Fields

Field Name	Field Description
Vsys-ID	Application identification number.
IP address	IPv4 address.
Port	Port number that are is use 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
```

show security idp attack table

Syntax show security idp attack table

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display detailed information of IDP attack table.

Required Privilege Level view

Related Topics attacks

clear security idp attack table

List of Sample Output show security idp attack table on page 1188

Output Fields Table 68 on page 1188 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 68: 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
```

show security idp counters application-ddos

Syntax show security idp counters application-ddos

Release Information Command introduced in Release 10.0 of JUNOS Software.

Description Display the status of all IDP application-ddos counter values.

Required Privilege Level view

Related Topics

List of Sample Output show security idp counters application-ddos on page 1190

Output Fields Table 69 on page 1189 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 69: 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 AppDDOS module.
App-DDOS processed packets	Number of total packets processed in the AppDDOS 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 AppDDoS module is disabled.
App-DDOS context values excluded	Number of context values excluded for actions, reporting, or both.
App-DDOS context value process succeeded	Number of times context value processing succeeded, including action and logging events if configured.

Table 69: show security idp counters application-ddos Output Fields *(continued)*

Field Name	Field Description
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
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 Software.

Description Display the status of all IDP application identification (AI) counter values.

Required Privilege Level view

Related Topics application (AppDDoS)

clear security idp counters application-identification

List of Sample Output show security idp counters application-identification on page 1192

Output Fields Table 70 on page 1191 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 70: 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.
AI-disabled sessions due to RPC match	Number of sessions disabled AI match due to RPC match.

Table 70: show security idp counters application-identification Output Fields *(continued)*

Field Name	Field Description
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 Software.

Description Display the status of all DFA counter values.

Required Privilege Level view

Related Topics clear security idp counters dfa

List of Sample Output show security idp counters dfa on page 1193

Output Fields Table 71 on page 1193 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 71: 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
```

show security idp counters flow

Syntax show security idp counters flow

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display the status of all IDP flow counter values.

Required Privilege Level view

Related Topics flow (IDP)

clear security idp counters flow

List of Sample Output show security idp counters flow on page 1195

Output Fields Table 72 on page 1194 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 72: 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.
Policy cache misses	Number of sessions that did not match policy cache.

Table 72: show security idp counters flow Output Fields *(continued)*

Field Name	Field Description
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 Packet Process	Number of packets processed from SM.
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
 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 Software.

Description Display the status of all IPS counter values.

Required Privilege Level view

Related Topics ips

clear security idp counters ips

List of Sample Output show security idp counters ips on page 1198

Output Fields Table 73 on page 1197 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 73: 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.
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.

Table 73: show security idp counters ips Output Fields *(continued)*

Field Name	Field Description
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 Software.

Description Display the status of all IDP log counter values.

Required Privilege Level view

Related Topics event-rate

clear security idp counters log

List of Sample Output show security idp counters log on page 1200

Output Fields Table 74 on page 1199 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 74: 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.

Table 74: 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
```

show security idp counters packet

Syntax show security idp counters packet

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display the status of all IDP packet counter values.

Required Privilege Level view

Related Topics clear security idp counters packet

List of Sample Output show security idp counters packet on page 1203

Output Fields Table 75 on page 1202 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 75: show security idp counters packet Output Fields

Field Name	Field Description
Processed packets	Number of packets processed by IDP service.
Dropped packets	Number of packets dropped by IDP service.
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.
GTP flows (Unsupported)	Number of GTP flows.
TCP decompression uncompressed IP (Unsupported)	Number of uncompressed IP headers that are to be TCP decompressed.

Table 75: show security idp counters packet Output Fields *(continued)*

Field Name	Field Description
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 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 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.

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 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 policy-manager

Syntax show security idp counters policy-manager

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display the status of all IDP policies counter values.

Required Privilege Level view

Related Topics clear security idp counters policy-manager

List of Sample Output show security idp counters policy-manager on page 1205

Output Fields Table 76 on page 1205 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 76: 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
```

show security idp counters tcp-reassembler

Syntax show security idp counters tcp-reassembler

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display the status of all TCP reassembler counter values.

Required Privilege Level view

Related Topics re-assembler

clear security idp counters tcp-reassembler

List of Sample Output show security idp counters tcp-reassembler on page 1207

Output Fields Table 77 on page 1206 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 77: 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.
New segments with no overlaps with old segment	Number of new segments that do not overlap with old segment.

Table 77: show security idp counters tcp-reassembler Output Fields *(continued)*

Field Name	Field Description
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
 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 Software.

Description Display the status of all IDP data plane memory.

Required Privilege Level view

List of Sample Output show security idp memory on page 1209

Output Fields Table 78 on page 1209 lists the output fields for the show security idp memory command. Output fields are listed in the approximate order in which they appear.

Table 78: show security idp memory Output Fields

Field Name	Field Description
PIC	Name of the PIC.
Total IDP data plane memory	Total memory space which 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 : spu-13
  Total IDP data plane memory : 307 MB
                           Used : 42 MB ( 43008 KB )
                      Available : 265 MB ( 271360 KB )
                            PIC : spu-12
  Total IDP data plane memory : 307 MB
                           Used : 42 MB ( 43008 KB )
                      Available : 265 MB ( 271360 KB )
```

show security idp security-package-version

Syntax show security idp security-package-version

Release Information Command introduced in Release 9.2 of JUNOS Software.

Description Display information of the currently installed security package version and detector version.

Required Privilege Level view

Related Topics security-package

request security idp security-package download

request security idp security-package install

List of Sample Output show security idp security-package-version on page 1210

Output Fields Table 79 on page 1210 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 79: 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 Software.

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 1211
show security idp ssl-inspection key key2 on page 1211

Output Fields Table 80 on page 1211 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 80: 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
```

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 Software.

Description Display all the SSL session IDs in the session ID cache. Each cache entry is 32 bytes long.

Required Privilege Level view

Related Topics clear security idp ssl-inspection session-id-cache

List of Sample Output show security idp ssl-inspection session-id-cache on page 1212

Output Fields Table 81 on page 1212 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 81: 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 Software.

Description Display the status of the current IDP policy.

Required Privilege Level view

List of Sample Output show security idp status on page 1213

Output Fields Table 82 on page 1213 lists the output fields for the show security idp status command. Output fields are listed in the approximate order in which they appear.

Table 82: 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.
Current policy	Name of the current installed policy.

show security idp status

```
user@host> show security idp status
Status of IDP: s0,      Up since: 2008-03-31 16:33:22 PDT (12:47:45 ago)
Packets/second: 0               Peak: 12 @ 2008-03-31 18:45:39 PDT
KBits/second  : 0               Peak: 6 @ 2008-03-31 18:45:39 PDT
Latency (microseconds): [min: 0] [max: 0] [ave: 0]
 Current policy: viking-policy v0
```

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 Software.

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 Topics
pre-shared-key

List of Sample Output
show security ike pre-shared-key on page 1214

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
```

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*>

Release Information Command introduced in Release 8.5 of JUNOS Software; fpc, pic, and kmd-instance options added in Release 9.3 of JUNOS Software.

Description Display information about Internet Key Exchange (IKE) security associations (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 IP 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 particular 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 (daemon) (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 IKE SAs in this particular PIC slot. This option is used to filter the output.

Required Privilege Level view

Related Topics clear security ike security-associations

List of Sample Output show security ike security-associations on page 1218
show security ike security-associations detail on page 1218
show security ike security-associations detail (SRX Series devices) on page 1219
show security ike security-associations index 8 detail on page 1219

show security ike security-associations 1.1.1.2 on page 1219
show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series devices) on page 1219

Output Fields Table 83 on page 1216 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 83: 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 the FPC slot-number and PIC slot-number. Currently, 4 kmd-instances 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 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 or 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.
Local	Address of the local peer.
Remote	Address of the remote peer.
Lifetime	Number of seconds remaining until the IKE SA expires.

Table 83: show security 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.
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.

Table 83: 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 Software 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

```
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 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
  Local identity: No Id
  Remote identity: No Id
  Flags: Caller notification sent, Waiting for remove
```

show security ike security-associations detail (SRX Series devices)

```
user@host> show security ike security-associations detaill
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
```

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 Software.

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 1220

Output Fields Table 84 on page 1220 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 84: 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*>

Release Information
Command introduced in Release 8.5 of JUNOS Software; fpc, pic, and kmd-instance options added in Release 9.3 of JUNOS Software.

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 particular Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.

index *SA-index-number*—(Optional) Display detailed information about the specified security association identified by 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 (daemon) (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 particular PIC slot. This option is used to filter the output.

Required Privilege Level
view

Related Topics
clear security ipsec security-associations

List of Sample Output
show security ipsec security-associations on page 1224
show security ipsec security-associations index on page 1224
show security ipsec security-associations brief on page 1225
show security ipsec security-associations detail on page 1225
show security ipsec security-associations detail (SRX Series devices) on page 1225
show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series devices on page 1225

Output Fields
Table 85 on page 1222 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 85: 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-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 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 security association is installed in the security association database. ■ Not Installed—The security association is not installed in the security association database. For transport mode, the value of State is always Installed.
Mon	The Mon refers to VPN monitoring status. If VPN monitoring is enabled, then this will show 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.
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 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.

Table 85: show security ipsec security-associations *(continued)*

Field Name	Field Description
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 the 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 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.
Mode	Mode of the security association: ■ transport—Protects host-to-host connections. ■ tunnel—Protects connections between security gateways.
Type	Type of the security association: ■ 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 security associations are not supported in transport mode.
State	State of the security association: ■ Installed—The security association is installed in the security association database. ■ Not Installed—The security association is not installed in the security association database. For transport mode, the value of State is always Installed.
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 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.
Hard lifetime	The hard lifetime specifies the lifetime of the SA. ■ Expires in seconds—Number of seconds left until the SA expires.

Table 85: show security ipsec security-associations *(continued)*

Field Name	Field Description
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

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID Gateway   Port  Algorithm    SPI   Life:sec/kb Sta vsys
5 5.5.5.4   500  esp:3des/sha1    ed0cec21   expir unlim I/I      0
5 5.5.5.4   500  esp:3des/sha1
```

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
```

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 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* >
pic *slot-number*

Release Information Command introduced in Release 8.5 of JUNOS Software; fpc and pic options added in Release 9.3 of JUNOS Software.

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 particular 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.

pic *slot-number* —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this particular PIC slot. This option is used to filter the output.

Required Privilege Level view

Related Topics clear security ipsec statistics

List of Sample Output show security ipsec statistics on page 1228
show security ipsec statistics index 5 on page 1228
show security ipsec statistics fpc 6 pic 1 (SRX Series devices) on page 1229

Output Fields Table 86 on page 1227 lists the output fields for the show security ipsec statistics command. Output fields are listed in the approximate order in which they appear.

Table 86: show security ipsec statistics Output Fields

Field Name	Field Description
Virtual-system	The root system.
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.

Table 86: show security ipsec statistics Output Fields *(continued)*

Field Name	Field Description
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
```

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 Software.

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 1 on page 1230
show security monitoring fpc 8 on page 1231

Output Fields Table 87 on page 1230 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 87: show security monitoring fpc fpc-number Output Fields

Field Name	Field Description
FPC	Slot number in which the FPC is installed. It can be between 0 to 11.
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).

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 %
```

show security nat destination pool

Syntax show security nat destination pool
< *pool-name* >
all

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 Topics pool (Destination NAT)

List of Sample Output show security nat destination pool dst-nat-pool1 on page 1232
show security nat destination pool all on page 1233

Output Fields Table 88 on page 1232 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 88: 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
```

show security nat destination rule

Syntax show security nat destination rule
<rule-name>
all

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 Topics rule (Destination NAT)

List of Sample Output show security nat destination rule r4 on page 1235
show security nat destination rule all on page 1235

Output Fields Table 89 on page 1234lists the output fields for the show security nat destination rule command. Output fields are listed in the approximate order in which they appear.Table 71 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 89: 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.
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.

Table 89: show security nat destination rule Output Fields *(continued)*

Field Name	Field Description
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
      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 Software.

Description Display a summary of Network Address Translation (NAT) destination pool information.

Required Privilege Level view

Related Topics pool (Destination NAT)

rule (Destination NAT)

List of Sample Output show security nat destination summary on page 1237

Output Fields Table 90 on page 1237 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 90: 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
```

```
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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics clear security nat incoming-table

List of Sample Output show security nat incoming-table on page 1240

Output Fields Table 91 on page 1239 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 91: 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.

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 Software; node options added in Release 9.0 of JUNOS Software.

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 1241

Output Fields Table 92 on page 1241 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 92: 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
```

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

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 Software.

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 Topics clear security nat source persistent-nat-table

List of Sample Output show security nat source persistent–nat–table all on page 1244
show security nat source persistent–nat–table internal-ip 10.10.10.197 on page 1244
show security nat source persistent–nat–table internal-ip 10.10.10.197 internal-port 6000 on page 1244
show security nat source persistent–nat–table interface on page 1244

Output Fields show security nat source persistent-nat-table 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 93: 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.
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
```

show security nat source pool

Syntax show security nat source pool
< *pool-name* >
all

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 Topics pool (Source NAT)

List of Sample Output show security nat source pool src-nat-pool1 on page 1245
show security nat source pool all on page 1246

Output Fields Table 94 on page 1245 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 94: 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.

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
```

show security nat source rule

Syntax show security nat source rule
<rule-name>
all

Release Information Command introduced in Release 9.2 of JUNOS Software.

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 Topics rule (Source NAT)

List of Sample Output show security nat source rule r1 on page 1248
show security nat source rule all on page 1248

Output Fields Table 95 on page 1247 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 95: 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.

Table 95: 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
```

```
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 Software.

Description Display a summary of Network Address Translation (NAT) source pool information.

Required Privilege Level view

Related Topics pool (Source NAT)

rule (Source NAT)

List of Sample Output show security nat source summary on page 1250

Output Fields Table 96 on page 1250 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 96: 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 is 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

    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 Software.

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 Topics rule (Static NAT)

List of Sample Output show security nat static rule rsr11 on page 1252
show security nat static rule all on page 1253

Output Fields Table 97 on page 1252 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 97: 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.

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 1254

Output Fields Table 98 on page 1254 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 98: 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
```

```
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 Software.

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 Topics ca-profile

request security pki ca-certificate verify

JUNOS System Basics and Services Command Reference

List of Sample Output show security pki ca-certificate ca-profile juniper brief on page 1257
show security pki ca-certificate ca-profile juniper detail on page 1258

Output Fields Table 99 on page 1256 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 99: 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.

Table 99: 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
    Serial number: 9998 7666 0817 5841 3062
```

```
Issuer:
  Common name: kpradeep.juniper.net
Subject:
  Organization: Juniper Netowrks, 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 rupudiation, 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 Software.

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 Topics clear security pki key-pair

JUNOS System Basics and Services Command Reference

List of Sample Output show security pki certificate-request certificate-id hassan brief on page 1261
show security pki certificate-request certificate-id hassan detail on page 1261

Output Fields Table 100 on page 1260 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 100: 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.
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption(1024 bits).

Table 100: show security pki certificate-request Output Fields *(continued)*

Field Name	Field Description
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 Software.

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 Topics crl

JUNOS System Basics and Services Command Reference

List of Sample Output show security pki crl ca-profile ca2 on page 1263
show security pki crl ca-profile ca2 brief on page 1263
show security pki crl ca-profile ca2 detail on page 1263

Output Fields Table 101 on page 1262 lists the output fields for the show security pki crl command. Output fields are listed in the approximate order in which they appear.

Table 101: 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.

Table 101: 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
```

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 Software.

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 Topics clear security pki local-certificate

request security pki local-certificate generate-self-signed

JUNOS System Basics and Services Command Reference

List of Sample Output show security pki local-certificate certificate-id on page 1265
show security pki local-certificate certificate-id detail on page 1266
show security pki local-certificate system-generated on page 1266
show security pki local-certificate system-generated detail on page 1266

Output Fields Table 102 on page 1264 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 102: 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.
Issued by	Authority that issued the digital certificate.

Table 102: show security pki local-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.
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
    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 Software.

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 Topics clear security policies statistics

List of Sample Output show security policies on page 1270
sshow security policies policy-name p1 detail on page 1270

Output Fields Table 103 on page 1268 lists the output fields for the show security policies command. Output fields are listed in the approximate order in which they appear.

Table 103: 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.
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.

Table 103: show security 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.
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.
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.

Table 103: show security policies Output Fields *(continued)*

Field Name	Field Description
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.

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: v-2-2-2-0
    Destination addresses: v-1-1-1-0
    Applications: any
    Action: permit, log, scheduled
  Policy: p2, State: enabled, Index: 5, Sequence number: 2
    Source addresses: v-2-2-2-0
    Destination addresses: v-1-1-1-0
    Applications: any
    Action: deny, scheduled
```

sshow security policies policy-name p1 detail

```
user@host> 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:
    v-2-2-2-0: 2.2.2.0/24
  Destination addresses:
    v-1-1-1-0: 1.1.1.0/24
  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
  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 Software; node options added in Release 9.0 of JUNOS Software.

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 1272
show security resource-manager group active 2048 on page 1272
show security resource-manager group active node primary on page 1272
show security resource-manager group active node all on page 1272
show security resource-manager group active 1024 node all on page 1272

Output Fields Table 104 on page 1271 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 104: 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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 1273
show security resource-manager resource active 8190 on page 1274
show security resource-manager resource active node local on page 1274
show security resource-manager resource active node primary on page 1274

Output Fields Table 105 on page 1273 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 105: 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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 1275
show security resource-manager settings node primary on page 1275
show security resource-manager settings node all on page 1276

Output Fields Table 106 on page 1275 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 106: 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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

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 Topics ids-option

List of Sample Output show security screen ids-option jscreen on page 1278
show security screen ids-option jscreen1 node all on page 1278

Output Fields Table 107 on page 1277 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 107: show security screen ids-option Output Fields

Field Name	Field Description
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 Transport Control Protocol (TCP) WinNuke attacks.
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.

Table 107: show security screen ids-option Output Fields *(continued)*

Field Name	Field Description
TCP SYN flood source threshold	Number of SYN segments to be received per second before the device starts 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 starts rejecting new connection requests.
ICMP large packet	Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes.

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
```

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 Software; node options added in Release 9.0 of JUNOS Software.

Description Display intrusion detection system (IDS) security screen statistics.

Options none—Display IDS security for all zones and interface.

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 Topics clear security screen statistics

clear security screen statistics interface

clear security screen statistics zone

List of Sample Output show security screen statistics zone scrzone on page 1281
show security screen statistics interface ge-0/0/3 on page 1282
show security screen statistics interface ge-0/0/1 node primary on page 1282

Output Fields Table 108 on page 1279 lists the output fields for the show security screen statistics command. Output fields are listed in the approximate order in which they appear.

Table 108: 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.
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.

Table 108: show security screen statistics Output Fields *(continued)*

Field Name	Field Description
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 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.
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.

Table 108: show security screen statistics Output Fields *(continued)*

Field Name	Field Description
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 Software 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.

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
  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
  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
  ICMP address 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 utm anti-spam statistics

Syntax show security utm anti-spam statistics

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Display antispam statistics for connections including total e-mail scanned, tagged and dropped connections.

Command is supported on J Series devices and SRX210, SRX240, and SRX650 devices.

Required Privilege Level view

Related Topics clear security utm anti-spam statistics

show security utm anti-spam status

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 Software.

Description Display antispam status for connections including whitelist and blacklist server information.

Required Privilege Level view

Related Topics clear security utm anti-spam statistics

show security utm anti-spam statistics

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
```

show security utm anti-virus statistics

Syntax show security utm anti-virus statistics

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Display antivirus statistics for connections including clean and infected files and scan engine status.

Required Privilege Level view

Related Topics clear security utm antivirus statistics

show security utm anti-virus status

request security utm anti-virus juniper-express-engine

request security utm anti-virus kaspersky-lab-engine

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 Software.

Description Display antivirus status for connections including clean and infected files and scan engine status.

Required Privilege Level view

Related Topics clear security utm antivirus statistics

show security utm anti-virus statistics

request security utm anti-virus juniper-express-engine

request security utm anti-virus kaspersky-lab-engine

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):
    ------------------------
    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 Software.

Description Display content-filtering statistics for connections including lists of blocked files and the reasons for blocking.

Required Privilege Level view

Related Topics clear security utm content-filtering statistics

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
```

show security utm session

Syntax show security utm session

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Display general UTM session information including all allocated sessions and active sessions.

Command introduced in Release 9.4 of JUNOS Software.

Required Privilege Level view

Related Topics clear security utm session

show security utm status

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 Software.

Description Display whether the UTM service is running or not.

Required Privilege Level view

Related Topics clear security utm session

show security utm session

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
```

show security utm web-filtering statistics

Syntax show security utm web-filtering statistics

Release Information Command introduced in Release 9.5 of JUNOS Software.

Description Display web-filtering statistics for connections including whitelist and blacklist hits and custom category hits.

Required Privilege Level view

Related Topics clear security utm web-filtering statistics

show security utm web-filtering status

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 Software.

Description Display whether the SurfControl CPA server is running or not.

Required Privilege Level view

Related Topics clear security utm web-filtering statistics

show security utm web-filtering statistics

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
```

show security zones

Syntax show security zones
<detail | terse>
< *zone-name* >

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics security-zone

List of Sample Output
show security zones on page 1293
show security zones abc on page 1294
show security zones abc detail on page 1294
show security zones terse on page 1294
show security zones my-shared-external on page 1294

Output Fields Table 109 on page 1293 lists the output fields for the show security zones command. Output fields are listed in the approximate order in which they appear.

Table 109: 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
Security zone: junos-global
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 0
   Interfaces:
```

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.
```

show security zones type

Syntax show security zones type
(functional | security)
<detail | terse>

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics security-zone

List of Sample Output
show security zones type functional on page 1295
show security zones type security on page 1296
show security zones type security terse on page 1296
show security zones type security detail on page 1296

Output Fields Table 110 on page 1295 lists the output fields for the show security zones type command. Output fields are listed in the approximate order in which they appear.

Table 110: 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:
Security zone: junos-global
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

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 Software.

Description Display a summary of the authentication table entries configured from the Infranet Controller. Authentication tables store mappings between JUNOS traffic flows and Unified Access Control (UAC) roles. The Infranet Controller uses the roles specified in the mappings to help determine the UAC policies to apply to the JUNOS flows.

Use this command when you have configured the SRX Series device to act as a JUNOS Enforcer in a UAC deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options detail—Displays a detailed view of all authentication table entries.

identifier *id*—Displays 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 1297
show services unified-access-control authentication-table detail on page 1297
show services unified-access-control authentication-table identifier 1 on page 1297

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
```

show services unified-access-control policies

Syntax show services unified-access-control policies

Release Information Command introduced in Release 9.4 of JUNOS Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's Infranet Controller.

Options detail—Displays a detailed view of all policies.

identifier *id*—Displays information about a specific policy by identification number.

Required Privilege Level view

List of Sample Output
show services unified-access-control policies on page 1298
show services unified-access-control policies detail on page 1298
show services unified-access-control policies identifier 1 on page 1298

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
```

show services unified-access-control status

Syntax show services unified-access-control status

Release Information Command introduced in Release 9.4 of JUNOS Software.

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 Enforcer in a Unified Access Control (UAC) deployment. When deployed as a JUNOS 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 1299

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
```

show system services dhcp client

Syntax show system services dhcp client
< *interface-name* >
<statistics>

Release Information Command introduced in Release 8.5 of JUNOS Software.

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 Topics dhcp

request system services dhcp

List of Sample Output show system services dhcp client on page 1301
show system services dhcp client ge-0/0/1.0 on page 1301
show system services dhcp client statistics on page 1302

Output Fields Table 111 on page 1300 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 111: 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.
Packets dropped	Total packets dropped.

Table 111: show system services dhcp client Output Fields *(continued)*

Field Name	Field Description
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
```

show system services dhcp relay-statistics

Syntax show system services dhcp relay-statistics

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Display information about the DHCP relay.

Required Privilege Level view and system

Related Topics dhcp

List of Sample Output show system services dhcp relay-statistics on page 1303

Output Fields Table 112 on page 1303 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 112: 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
```

show wan-acceleration status

Syntax show wan-acceleration status

Release Information Command introduced in Release 8.5 of JUNOS Software.

Description Display the redirection status and related information about the WXC Integrated Services Module (ISM 200) for WAN acceleration.

Required Privilege Level view

Related Topics request wan-acceleration login

[Unresolved xref]

List of Sample Output show wan-acceleration status on page 1305

Output Fields Table 113 on page 1305 lists the output fields for the show wan-acceleration status command. Output fields are listed in the approximate order in which they appear.

Table 113: 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 Software.
WXOS version	Installed version of WXOS.
JUNOS/WXOS protocol	Indicates whether the JUNOS Software 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 Software.

Description Display access point status information.

Options none—Displays the status of all access points on the services gateway.

name—(Optional) Displays information about a specific access point on the services gateway.

detail—(Optional) Displays detailed information about a specific access point on the services gateway.

virtual-access-points—(Optional) Displays information about the virtual access points configured on a specific access point on the services gateway.

client-associations—(Optional) Displays information about the client associations on a specific access point on the services gateway.

neighbors—(Optional) Displays information about the neighbor access points of a specific access point on the services gateway.

Required Privilege Level view

Output Fields Table 114 on page 1306 lists the output fields for the show wlan access-points command. Output fields are listed in the approximate order in which they appear.

Table 114: 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
```

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
```

Part 3
Index

■ Index on page 1311

Index

Symbols

#, comments in configuration statements.....xlii
( ), in syntax descriptions.....xlii
(antivirus utm-policy).....437
(content-filtering utm-policy).....419
< >, 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.....889
access-point-name statement.....129
access-point-options statement
    WLAN.....893
access-point-queues statement
    WLAN.....894
access-profile statement.....267
    (Dynamic VPNs).....267
    (IPsec VPNs).....267
Accounting-Options Configuration Statement Hierarchy.....37
ack-number statement.....268
action (web filtering).....271
action statement.....269, 270
activation-priority statement.....130
active-policy statement.....271
adaptive-shaper statement.....83
adaptive-shapers statement.....84
address (peer call server) statement.....775
address statement.....274, 775
    (ARP Proxy Services Gateway).....274
    (Destination NAT Services Gateway).....275
    (IKE Gateway).....275
    (Zone Address Book).....276
    (Zone Address Set).....276
address-blacklist.....277
address-book statement.....277
address-persistent statement.....278
address-set statement.....278
address-whitelist.....279
admin-email.....279
admin-search statement.....6
administrator statement.....280
aging statement.....280
alarm-threshold statement.....281
alarm-without-drop statement.....281
alert statement.....282
alg statement.....41, 283
algorithm statement.....287
all-day statement.....222
all-tcp statement.....287
allow-dns-reply statement.....288
allow-icmp-without-flow statement.....288
always-send statement.....289
analog (station-type) statement.....776
analog-template statement.....777, 841
annex.....130
anomaly statement.....289
antispam.....290
antispam (feature-profile).....290
antispam (utm-policy).....291
antivirus.....292
antivirus (feature-profile).....293
antivirus (utm-policy).....295
apn (gtp).....296
application AppDDoS.....297
application statement.....297
    (Protocol Binding Custom Attack).....297
    (Security Policies).....298
application-identification statement.....298
application-level DDoS rule statement.....606
application-protocol statement.....42
application-screen statement.....299
    (H323).....299
    (MGCP).....300
    (SCCP).....300
    (SIP).....301
application-services (maximize-idp-sessions).....302
application-services statement.....303
application-services statement (Unified Access Control).....303
application-system-cache statement.....304
application-system-cache-timeout statement.....304
Applications Configurations Statement Hierarchy.....39
arbitration-inter-frame-space statement
    WLAN.....895

assemble statement statement.....7
attack-threshold statement.....305
attack-type statement.....308
(Custom Attack).....308, 309, 310
attacks statement.....306
(Exempt Rulebase).....306
(IPS Rulebase).....307
auth-id (peer-call-server) statement.....778
auth-id (station) statement.....779
auth-password (peer-call-server) statement.....780
auth-password (station) statement.....781
authentication statement.....313
authentication-algorithm statement.....314
authentication-method statement.....131, 315
authentication-order statement 7
authorization statement.....862
auto-re-enrollment statement.....316
automatic statement.....316

B

background-queue statement
WLAN.....895
banner statement.....8
(FTP, HTTP, Telnet).....8
(Web Authentication).....9
base-distinguished-name statement.....9
beacon-interval statement
WLAN.....896
bearer-bandwidth-limit statement.....131
best-effort-queue statement
WLAN.....896
bind-interface statement.....317
block-command.....317
block-content-type.....318
block-mime.....318
braces, in configuration statements.....xlii
brackets
angle, in syntax descriptions.....xli
square, in configuration statements.....xlii
bridge domain
routing interface.....56
VLAN identifier.....57
VLAN identifier list.....58
bridge statement.....319
Bridge-Domains Configuration Statement
Hierarchy.....53
bridge-domains statement.....54
bridge-options statement.....55
broadcast-multicast-rate-limit statement
WLAN.....897
bundle statement.....132

C

c-timeout statement.....320
ca-identity statement.....320
ca-profile statement.....321, 783
ca-profile-name statement.....322
cache.....322
cache-size statement.....323
call-flood statement.....323
call-type (policy) statement.....785
caller-id-transmit statement (analog and sip
templates).....784
cas-group statement.....789
category (web filtering).....325
category statement.....324
(Security Logging).....324
cellular-options statement.....133
certificate statement.....325
certificate-id statement.....326
chain statement.....327
challenge-password statement.....328
channel statement
WLAN.....897
Chassis Configuration Statement Hierarchy.....59
class-of-restriction (analog template, sip
template).....793
Class-of-Service Configuration Statement
Hierarchy.....79
clear chassis cluster control-plane statistics
command.....936
clear chassis cluster data-plane statistics
command.....937
clear chassis cluster failover-count command.....938
clear chassis cluster statistics command.....939
clear esis adjacency command.....940
clear esis statistics command.....941
clear gtp tunnels command.....943
clear network-access requests pending
command.....942
clear network-access requests statistics
command.....944
clear network-access securid-node-secret-file
command.....945
clear security alg h323 counters command.....946
clear security alg mgcp calls command.....947
clear security alg mgcp counters command.....948
clear security alg msrpc portmap command.....949
clear security alg sccp calls command.....950
clear security alg sccp counters command.....951
clear security alg sip calls command.....952
clear security alg sip counters command.....953
clear security alg sunrpc portmap
command.....954, 955
clear security datapth-debug counters command.....956
clear security firewall-authentication history address
command.....958
clear security firewall-authentication history
command.....957

clear security firewall-authentication history identifier command....959
clear security firewall-authentication users address command....961
clear security firewall-authentication users command....960
clear security firewall-authentication users identifier command....962
clear security flow session all command....963
clear security flow session application command....964
clear security flow session destination-port command....966
clear security flow session destination-prefix command....967
clear security flow session interface command....968
clear security flow session protocol command....969
clear security flow session resource-manager command....971
clear security flow session session-identifier command....972
clear security flow session source-port command....973
clear security flow session source-prefix command....974
clear security idp application-identification application-system-cache command....975
clear security idp attack table command....976
clear security idp counters application-identification command....977
clear security idp counters dfa command....978
clear security idp counters flow command....979
clear security idp counters ips command....980
clear security idp counters log command....981
clear security idp counters packet command....982
clear security idp counters policy-manager command....983
clear security idp counters tcp-reassembler command....984
clear security idp ssl-inspection session-id-cache command....985
clear security ike respond-bad-spi-count command....986
clear security ike security-associations command....987
clear security ipsec security-associations command....989
clear security ipsec statistics command....990
clear security nat incoming-table command....991
clear security nat source persistent-nat-table command....992
clear security pki key-pair command....993
clear security pki local-certificate command....994
clear security policies statistics command....995
clear security screen statistics command....996
clear security screen statistics interface command....997
clear security screen statistics zone command....998
clear security utm anti-spam statistics....999
clear security utm antivirus statistics....1000
clear security utm content-filtering statistics....1001
clear security utm session....1002
clear security utm web-filtering statistics....1003
clear-threshold statement....328
client-group statement....10
client-identifier statement....134
client-idle-timeout statement....10
client-list-name statement....862
client-name-filter statement....11
client-session-timeout statement....11
clients statement....329
cluster statement....63
code statement....330
code-point statement....84
comments, in configuration statements....xlii
compression-device statement....134
condition statement....167
configuration-file statement....12
connection-flood statement....331
connection-rate-threshold statement....330
connections-limit statement....331
console statement
  WLAN....898
container statement....332
content-filtering....333
content-filtering (utm-policy)....334
content-size....334
content-size-limit....335
context statement....335, 336
control-link-recovery statement....64
control-ports statement....65
conventions
  notice icons....xl
  text and syntax....xli
corrupt-file....336
count statement....12, 337
  (Custom Attack)....337
  (Security Policies)....337
country statement
  WLAN....899
crl statement....338
curly braces, in configuration statements....xlii
custom-attack statement....339
custom-attack-group statement....343
custom-attacks statement....343
custom-block-message....344
custom-message....345
custom-message (antivirus notification-options fallback-block/non-block)....345
custom-message (antivirus notification-options virus-detection)....345
custom-message (antivirus pattern-update email-notify)....348
custom-message-subject....347

custom-message-subject (antivirus notification-options fallback-block/non-block).....347
custom-message-subject (antivirus notification-options virus-detection).....347
custom-objects.....349
custom-tag-string.....349
custom-url-category.....350
customer support.....xlii
contacting JTAC.....xlii

D

daily statement.....223
data-length statement.....350
dead-peer-detection statement.....352
decompress-layer.....352
decompress-layer-limit.....353
default.....354
default (antivirus fallback-options).....354
default (web-filtering fallback-settings).....355
default statement.....85
default-policy statement.....355
default-profile statement.....13
deny statement.....356
(Policy).....356
(SIP).....357
description (peer call server) statement.....795
description (trunk groups) statement.....796
description statement.....358
(IDP Policy).....358
(Security Policies).....358
destination statement.....359
(Destination NAT Services Gateway).....359
(IP Headers in Signature Attack).....360
destination-address statement.....361
(Destination NAT Services Gateway).....361
(IDP Policy).....362
(Security Policies).....362
(Source NAT Services Gateway).....363
(Traffic Policy Services Gateway).....364
destination-except statement.....364
destination-ip statement.....365
destination-ip-based statement.....365
destination-nat statement
(Destination NAT Services Gateway).....366
destination-port statement.....43, 367
(Destination NAT Services Gateway).....367
(Signature Attack).....367
destination-threshold statement.....368
detect-shellcode statement.....368
detector statement.....369
df-bit statement.....369
dh-group statement.....370
dhcp statement.....135
digit-transform statement (digit-manipulation).....800
digit-transform statement (trunk-group).....800
direct-inward-dialing statement.....801
direct-inward-line statement.....801
direction statement.....371
(Custom Attack).....371
(Dynamic Attack Group).....372
directory (music-on-hold) statement.....802
disable statement.....158
ES-IS.....192, 193
disable-call-id-hiding statement.....372
disable-dot11d statement
WLAN.....900
distinguished-name statement.....13, 373
dns statement.....374
documentation
comments on.....xlii
domain-name statement.....14
domain-type statement.....55
dot1x statement
WLAN.....901
dot1x-supplicant statement
WLAN.....902
download-profile.....375
download-profile (ftp antivirus utm-profile).....375
download-profile (ftp content-filtering utm-profile).....375
drop (gtp).....376
dtim-period statement
WLAN.....902
dtmf-method statement (peer call server, sip template).....803
duration statement.....158
dynamic statement.....379
dynamic-attack-group statement.....381
dynamic-call-admission-control statement.....136
dynamic-vpn statement.....380

E

early-ageout statement.....382
email-notify.....382
enable-all-qmodules statement.....383
enable-packet-pool statement.....383
encapsulation statement.....137
encryption statement.....384
encryption-algorithm statement.....385
end-system-configuration-timer statement
ES-IS.....192
endpoint-registration-timeout statement.....385
engine-not-ready.....386
enrollment statement.....387
esis statement.....193
establish-tunnels statement.....388
ethernet statement
WLAN.....905
Event-Options Configuration Statement Hierarchy.....101

event-rate statement....388
exception....389
exception (antivirus mime-whitelist)....389
exception (content-filter block-mime)....389
exclude statement....224
exclude-context-values statement....390
expression statement....391
extension statement (live-attendant)....804
extension statement (station)....807
extension-inherit statement....805
extension-number statement (voicemail)....806
external statement
WLAN....903
external-interface statement....392
(IKE Gateway)....392
(Manual Security Association)....392

F

fabric-options statement....138
fail statement....14
fallback-block....393
fallback-options....394
fallback-options (antivirus
juniper-express-engine)....394
fallback-options (antivirus kaspersky-lab-engine)....395
fallback-settings....396
fallback-settings (web-filtering juniper-local)....397
fallback-settings (web-filtering
surf-control-integrated)....396
fallback-settings (web-filtering
websense-redirect)....397
false-positives statement....398
family bridge statement....139
family statement....399
feature-profile....400
features statement....808
filename-extension....403
filters statement....404
fin-no-ack statement....405
Firewall Configuration Statement Hierarchy....103
firewall filters
statistics
clearing 1215
displaying....1293, 1300
firewall-authentication statement....15, 406
(Policies)....406
(Security)....407
firewall-authentication-service statement....873
firewall-user statement....16
fixed-multicast-rate statement
WLAN....904
flood statement....408
(ICMP)....408
(UDP)....409
flow statement....410
(IDP)....410
(Security Flow)....411
flow-control statement....140
font conventions....xli
force-upgrade statement....412
format (music-on-hold) statement....809
format statement, first use....412
format statement, second use....413
Forwarding-Options Configuration Statement
Hierarchy....109
forwarding-options statement....413
forwarding-process....414
fragment statement....414
fragmentation-threshold statement
WLAN....904
friday statement....225
from statement....415, 809
from-zone statement....416
(IDP Policy)....416
(Security Policies)....417
ftp (antivirus utm-policy)....419
ftp (utm)....419
ftp statement....16, 418
functional-zone statement....420

G

gatekeeper statement....421
gateway statement....422
(IKE)....423
(IPsec)....424
(Manual Security Association)....424
general-authentication-service statement....874
Gi interface....430
global-mac-limit statement....195
global-mac-table-aging-time statement....195
global-no-mac-learning statement....196
Gp interface....430
gprs statement....428
graceful-restart statement
ES-IS....193
gratuitous-arp-count statement....66
gre-in statement....425
gre-out statement....426
group-members statement....427
Groups Configuration Statement Hierarchy....115
gsm-options statement....141
gtp statement....428
guard-band statement....159

H

h323 statement....431
hardware
supported platforms....xxxviii

header-length statement....432
heartbeat-interval statement....66
heartbeat-interval-normal statement....810
heartbeat-survivable interval statement....810
heartbeat-threshold statement....67
high-watermark statement....434
hit-rate-threshold statement....433
hold-down-interval statement....67
hold-time statement
ES-IS....194
host....434
host (Security Logging) statement....435
host-address-base statement....435
host-inbound-traffic statement....436
hostname statement....436
hours statement....811
http statement....17
http-profile....437
http-profile (content-filtering utm-policy)....437
http-profile (web-filtering utm-policy)....438
http-redirect statement
WLAN....905

I

icmp statement....439
(Protocol Binding Custom Attack)....439
(Security Screen)....440
(Signature Attack)....441
icmp-code statement....46
icmp-type statement....47
identification statement....442
(ICMP Headers in Signature Attack)....442
(IP Headers in Signature Attack)....443
idle-time statement....443
idp statement....444
idp-policy statement....451
ids-option statement....453
ignore-mem-overflow statement....454
ignore-regular-expression statement....455
ike statement....456
(IPsec VPN)....456
(Security)....457
ike-policy statement....458
ike-user-type statement....459
imap-profile....460
imap-profile (antivirus utm-policy)....460
imap-profile (content-filtering utm-policy)....460
IMSI prefix (gtp)....510
inactive-media-timeout statement....461
(MGCP)....461
(SCCP)....461
(SIP)....462
inactivity-timeout statement....47
include-destination-address statement....462
inet statement....463
inet6 statement....463
infranet-controller statement....813
install-interval statement....464
intelligent-prescreening....464
interface statement....160, 465, 814
(ARP Proxy Services Gateway)....465
(source NAT)....465
bridge domain....56
ES-IS....194
interface-monitor statement....68
Interfaces Configuration Statement Hierarchy....117
interfaces statement....466
interval (anti-virus)....468
interval (juniper-express-engine)....468
interval (kaspersky-lab-engine)....468
interval statement....160, 467, 815
(IDP)....467
(IKE)....467
ip statement....469
(Protocol Binding Custom Attack)....469
(Security Screen)....470
(Signature Attack)....472
ip-action statement....473
application-level DDoS....474
ip-block statement....474
ip-close statement....475
ip-flags statement....475
ip-monitoring statement....69
ip-notify statement....476
ip-sweep statement....479
ips statement....476
ipsec-policy statement....477
ipsec-vpn statement....478
(Dynamic VPNs)....479
(Flow)....478
(Policies)....478
iso statement....480

J

juniper-express-engine....481
juniper-local....482

K

kaspersky-lab-engine....483

L

l2-learning statement....196
land statement....484
large statement....484
ldap-options statement....18
ldap-server statement....19
lease-time statement....142
lifetime-kilobytes statement....485

limit....485
limit-session statement....486
link-speed statement....143
list....487
list (antivirus mime-whitelist)....487
list (content-filter block-mime)....487
live-attendant statement....816
local statement....488
local-certificate statement....488
local-identity statement....489
log statement....490
(GTP)....491
(IDP Policy)....492
(IDP)....492
(Security Logging)....494
(Security Policies)....493
log-attacks statement....495
log-errors statement....495
log-supercede-min statement....496
login statement....19
loopback statement....143
low-watermark statement....496

M

mac-authentication-type statement
WLAN....906
management statement....161, 497
management-vlan statement
WLAN....906
manual statement....498
manuals
comments on....xlii
match statement....499
(Destination NAT Services Gateway)....499
(IDP Policy)....500, 501
(Security Policies)....501
(Source NAT Services Gateway)....502
max-context-values statement....503
max-flow-mem statement....503
max-logs-operate statement....504
max-packet-mem statement....505
max-packet-memory statement....505
max-sessions statement....506
max-tcp-session-packet-memory statement....506
max-time-report statement....507
max-timers-poll-ticks statement....507
max-udp-session-packet-memory statement....508
maximize-idp-sessions....508
maximum-burst statement
WLAN....907
maximum-call-duration statement....509
maximum-contention-window statement
WLAN....908
maximum-power statement....161
maximum-stations statement
WLAN....907
max–message-length (gtp)....504
mcc-mnc (gtp)....510
media-gateway statement....817
media-source-port-any statement....511
member statement....511
member-interfaces statement....144
message-flood statement....512
(H323)....512
(MGCP)....513
mgcp statement....514
mime-pattern....515
mime-whitelist....515
minimum-contention-window statement
WLAN....908
min–message-length (gtp)....516
mode (Security Logging) statement....518
mode statement....517
(Forwarding Options)....517
(Policy)....517
WLAN....909
monday statement....226
monitor-timeout statement....818
mpls statement....518
msrpc statement....519
mss statement....520
music-on-hold statement....819

N

name-server statement
WLAN....909
nat statement
(Services Gateway Configuration)....521
nat-keepalive statement....523
native-vlan-id statement....144
negate statement....523
network-security statement....875
next-hop statement....819
next-hop-tunnel statement....145
no-acknowledgement statement
WLAN....910
no-allow-icmp-without-flow statement....524
no-anti-replay statement....524
no-auto-power-save statement
WLAN....910
no-broadcast-ssid statement
WLAN....911
no-enable-all-qmodules statement....524
no-enable-packet-pool statement....524
no-flow-control statement....145
no-log-errors statement....524
no-loopback statement....145
no-nat-traversal statement....525
no-policy-lookup-cache statement....525

no-reset-on-policy statement....525
no-sequence-check statement....525
no-short-guard-interval-supported statement
WLAN....911
no-source-filtering statement....145
no-syn-check statement....526
no-syn-check-in-tunnel statement....526
no-wifi-multimedia statement
WLAN....911
node statement....70
(Cluster)....70
(Redundancy-Group)....70
notice icons....xl
notification statement....527
notification-options....528
notification-options (antivirus
juniper-express-engine)....528
notification-options (antivirus
kaspersky-lab-engine)....529
notification-options (content-filtering)....529
notify-mail-sender....530
notify-mail-sender (antivirus fallback-block)....530
ntp-sever statement
WLAN....912

O

optimized statement....531
option statement....531
order (music-on-hold) statement....820
order statement....532
out-of-resources....532
over-limit....533
overflow-pool statement
;(Source NAT Services Gateway....533

P

packet-action statement....197
pair-policy statement....535
parentheses, in syntax descriptions....xlii
pass-through statement....20, 536
password statement....21, 820
password-file....537
pattern statement....537
pattern update....538
pattern-update (juniper-express-engine)....539
pattern-update (kaspersky-lab-engine)....538
peer-call-server (media gateway) statement....822
peer-call-server statement....821, 823
peer-certificate-type statement....539
peer-proxy-server....822
perfect-forward-secrecy statement....540
performance statement....541
permission statement....823
permit statement....542
permit-command....543
persistent-nat statement....544
pic-mode....146
pic-mode statement....71
ping-death statement....545
pki statement....546
pki-local-certificate statement....875
PoE configuration statement hierarchy....157
policers, displaying....1268
policies statement....548
policy statement....550
(IKE)....550
policy statement (survivable call server)....824
policy statement: (Security)....552
policy-lookup-cache statement....553
Policy-Options Configuration Statement
Hierarchy....165
policy-rematch statement....553
pool statement....554
(Destination NAT Services Gateway)....554
(Source NAT Services Gateway)....555
pool-utilization-alarm statement....555
pop3-profile (antivirus utm-policy)....556
pop3-profile (content-filtering utm-policy)....556
pop3–profile....556
port (reverse ssh)....876
port (reverse telnet)....876
port (web filtering)....557
port statement....22, 557, 825
(LDAP)....22
(RADIUS)....22
port-randomization statement
(source NAT)....558
port-scan statement....559
pptp statement....560
pre-filter-shellcode statement....560
pre-shared-key statement....562
predefined-attack-groups statement....561
predefined-attacks statement....561
preempt statement....71
preference statement
ES-IS....197
priority statement....72, 162
process-ignore-s2c statement....562
process-override statement....563
process-port statement....563
processes
restarting....1038
products statement....564
profile....565
profile (antispam sbl)....565
profile (antivirus juniper-express-engine)....567
profile (antivirus kaspersky-lab-engine)....566
profile (content-filtering)....568
profile (gtp)....569
profile (web-filtering juniper-local)....573

profile (web-filtering surf-control-integrated).....571
profile (web-filtering websense-redirect).....572
profiles statement.....146
propagate-settings statement.....877
proposal statement.....574
proposal-set statement.....575
(IKE).....575
(IPsec).....576
protect statement.....577
protection statement
WLAN.....912
protocol statement.....48, 578, 826
(IP Headers in Signature Attack).....579
(IPsec).....578
(Manual Security Association).....578
(Signature Attack).....580
protocol-binding statement.....583
protocol-command.....584
protocol-name statement.....584
Protocols Configuration Statement Hierarchy.....169
protocols statement.....585
(Interface Host-Inbound Traffic).....586
(Zone Host-Inbound Traffic).....588
proxy-arp statement
(Services Gateway Configuration).....589
proxy-identity statement.....589
pstn-access-number statement 827

Q

quality-of-service statement
WLAN.....913

R

radio statement
WLAN.....915
radio-off statement
WLAN.....917
radio-options statement
WLAN.....918
radius-options statement.....23
radius-server statement.....24
raise-threshold statement.....590
rate-limit (gtp).....590
re-assembler statement.....592
re-enroll-trigger-time-percentage statement.....592
real statement.....591
recommended statement.....593
recommended-action statement.....594
redundancy-group statement.....73, 147
redundant-ether-options statement.....147
redundant-parent statement.....148
(Fast Ethernet Options).....148
(Gigabit Ethernet Options).....148
regexp statement.....594
registration-expiry-timeout statement.....827
regular-expression statement.....828
reject statement.....595
reject-timeout statement.....595
remote statement.....596
remote-exceptions statement.....596
remote-protected-resources statement.....597
remove-r6 (gtp).....597
request chassis cluster failover node command.....1006
request chassis cluster failover reset command.....1007
request modem wireless activate iota
command.....1008
request modem wireless activate manual
command.....1009
request modem wireless activate otasp
command.....1011
request modem wireless gsm sim-unblock
command.....1012
request modem wireless gsm sim-unlock
command.....1013
request security datapath-debug capture start
command.....1014
request security datapath-debug capture stop
command.....1015
request security idp security-package download
command.....1016
request security idp security-package install
command.....1018
request security idp ssl-inspection key add
command.....1019
request security idp ssl-inspection key delete
command.....1021
request security pki ca-certificate verify
command.....1022
request security pki local-certificate generate-self-signed
command.....1023
request security pki local-certificate verify
command.....1025
request security utm anti-virus
juniper-express-engine.....1026
request security utm anti-virus
kaspersky-lab-engine.....1027
request system license update command.....1028
request system partition compact-flash
command.....1029
request system services dhcp command.....1030
request system software in-service-upgrade
command.....1031
request wan-acceleration login command.....1033
request wlan access-point firmware upgrade
command.....1034
request wlan access-point restart command.....1035
reset statement.....598
reset-on-policy statement.....598
respond-bad-spi statement.....599
restart command.....1038

restart-duration statement
ES-IS....193
restarting
software processes....1038
retain-hold-resource statement....599
reth-count statement....74
retransmission-attempt statement....149
retransmission-interval statement....149
retry statement....25
(LDAP)....25
(RADIUS)....25
reverse ssh....877
reverse telnet....878
revert-interval statement....26
(LDAP)....26
(RADIUS)....26
revocation-check statement....600
ring-count statement....829
roaming-mode statement....150
route statement (route-policy)....831
route-active-on statement....167
route-change-timeout statement....600
route-pattern statement....830
route-policy statement....832
routing-instance statement....601
(Destination NAT Services Gateway)....601
(LDAP)....27
(RADIUS)....27
(Source NAT Services Gateway)....601
Routing-Instances Configuration Statement Hierarchy....201
routing-interface statement....56
Routing-Options Configuration Statement Hierarchy....213
rpc statement....602
rpc-program-number statement....49
rsh statement....603
rst-invalidate-session statement....604
rst-sequence-check statement....604
rts-threshold statement
WLAN....919
rtsp statement....605
rule statement....606
(destination NAT)....607
(Exempt Rulebase)....608
(IPS Rulebase)....609
(Source NAT)....610
DDoS Rulebase....606
rule-set statement....613
(Destination NAT Services Gateway)....613
(Source NAT Services Gateway)....614
rulebase-ddos statement....612
rulebase-exempt statement....616
rulebase-ips statement....617

S

saturday statement....227
sbl....618
sbl-default-server....619
scan-mode....619
scan-options....620
scan-options (anti-virus kaspersky-lab-engine)....621
scan-options (antivirus juniper-express-engine)....620
sccp statement....622
scheduler statement....228
scheduler-name statement....623
Schedulers Configuration Statement Hierarchy....221
schedulers statement....229
scope statement....624
(Chain Attack)....624
(Custom Attack)....625
screen statement....626
(Security)....627
(Zones)....628
search statement....28
search-filter statement....28
secret statement....29
securid-server statement....29
Security Configuration Statement Hierarchy....237
security statement
WLAN....920
security-package statement....629
security-zone statement....630
select-profile statement....150
sensor-configuration statement....631
separator statement....30
seq-number-validated (gtp)....632
sequence-number statement....636
(ICMP Headers in Signature Attack)....636
(TCP Headers in Signature Attack)....637
server....633
server-address statement....151
server-certificate-subject statement....833
server-connectivity....633
service statement....638
(Anomaly Attack)....638
(DDoS)....638
(Dynamic Attack Group)....639
(Security IPsec)....639
service-point statement....833
Services Configuration Statement Hierarchy....773
session-close statement....634
session-init statement....635
session-options statement....30
sessions statement....634
sessions-per-client....635
severity statement....640
(Custom Attack)....640
(Dynamic Attack Group)....641
(IPS Rulebase)....642
shellcode statement....643

show bgp neighbor command.....1040
show chassis cluster control-plane statistics command.....1044
show chassis cluster data-plane statistics command.....1046
show chassis cluster interfaces command.....1048
show chassis cluster ip-monitoring status redundancy-group command.....1050
show chassis cluster statistics command.....1052
show chassis cluster status command.....1056
show chassis fpc command.....1059
show chassis hardware command.....1062
show esis adjacency command.....1067
show esis interface command.....1069
show esis statistics command.....1071
show ethernet-switching mac-learning-log command.....1072
show ethernet-switching table command.....1074
show gtp tunnels.....1078
show igmp-snooping route command.....1079
show igmp-snooping vlans command.....1081
show interfaces command.....1083
show interfaces flow-statistics command.....1089
show modem wireless interface command.....1091
show modem wireless interface firmware command.....1093
show modem wireless interface network command.....1095
show modem wireless interface rssi command.....1097
show network-access requests pending command.....1098
show network-access requests statistics command.....1100
show network-access securid-node-secret-file command.....1101
show poe controller command.....1102
show poe interface command.....1103
show poe telemetries interface.....1105
show schedulers command.....1107
show security alg h323 counters command.....1109
show security alg mgcp calls command.....1111
show security alg mgcp counters command.....1113
show security alg mgcp endpoints command.....1115
show security alg msrpc command.....1117
show security alg sccp calls command.....1119
show security alg sccp counters command.....1121
show security alg sip calls command.....1123
show security alg sip counters command.....1126
show security alg sip rate command.....1130
show security alg sip transactions command.....1131
show security alg status command.....1132
show security alg sunrpc portmap command.....1134
show security datapath-debug capture.....1135, 1136
show security datapath-debug counter.....1137
show security dynamic-vpn client version.....1138
show security dynamic-vpn users.....1139
show security dynamic-vpn users terse.....1140
show security firewall-authentication history address command.....1143
show security firewall-authentication history command.....1141
show security firewall-authentication history identifier command.....1146
show security firewall-authentication users address command.....1150
show security firewall-authentication users command.....1148
show security firewall-authentication users identifier command.....1152
show security flow gate command.....1154
show security flow session application command.....1159
show security flow session command.....1157
show security flow session destination-port command.....1161
show security flow session destination-prefix command.....1163
show security flow session interface command.....1165
show security flow session protocol command.....1167
show security flow session resource-manager command.....1170
show security flow session session-identifier command.....1172
show security flow session source-port command.....1176
show security flow session source-prefix command.....1178
show security flow session summary command.....1180
show security flow session tunnel command.....1182
show security idp active-policy command.....1184
show security idp application-ddos command.....1185
show security idp application-identification application-system-cache command.....1187
show security idp attack table command.....1188
show security idp counters application-ddos command.....1189
show security idp counters application-identification command.....1191
show security idp counters dfa command.....1193
show security idp counters flow command.....1194
show security idp counters ips command.....1197
show security idp counters log command.....1199
show security idp counters packet command.....1202
show security idp counters policy-manager command.....1205
show security idp counters tcp-reassembler command.....1206
show security idp memory command.....1209
show security idp security-package-version command.....1210
show security idp ssl-inspection key command.....1211

show security idp ssl-inspection session-id-cache command....1212
show security idp status command....1213
show security ike pre-shared-key command....1214
show security ike security-associations command....1215
show security ipsec next-hop-tunnels command....1220
show security ipsec security-associations command....1221
show security ipsec statistics command....1227
show security monitoring fpc fpc-number command....1230
show security nat destination pool command....1232
show security nat destination rule command....1234
show security nat destination summary command....1237
show security nat incoming-table command....1239
show security nat interface-nat-ports command....1241
show security nat source persistent-nat-table command....1243
show security nat source pool command....1245
show security nat source rule command....1247
show security nat source summary command....1250
show security nat static-nat summary command....1254
show security pki ca-certificate command....1256
show security pki certificate-request command....1260
show security pki crl command....1262
show security pki local-certificate command....1264
show security policies command....1268
show security resource-manager group active command....1271
show security resource-manager resource active command....1273
show security resource-manager settings command....1275
show security screen ids-option command....1277
show security screen statistics command....1279
show security utm anti-spam statistics....1284
show security utm anti-spam status....1285
show security utm anti-virus statistics....1286
show security utm anti-virus status....1287
show security utm content-filtering statistics....1288
show security utm session....1289
show security utm status....1290
show security utm web-filtering statistics....1291
show security utm web-filtering status....1292
show security zones command....1293
show security zones type command....1295
show services unified-access-control authentication-table command....1297
show services unified-access-control policies command....1298
show services unified-access-control status command....1299
show system services dhcp client command....1300
show system services dhcp relay-statistics command....1303
show wan-acceleration status command....1305
show wlan access-points command....1306
signature statement....644
sip statement....648
sip statement (media gateway, peer call server, survivable call server)....834
sip-password statement....152
sip-template statement....841
sip-template statement (station type)....835
sip-timeout statement....836
sip-user-id statement....152
smtp-profile....649
smtp-profile (antispam utm-policy)....649
smtp-profile (antivirus utm-policy)....649
smtp-profile (content-filtering utm-policy)....650
SNMP Configuration Statement Hierarchy....857
sockets....650
source statement....651
(IP Headers in Signature Attack)....651
(Source NAT Services Gateway)....652
source-address statement....31, 654
(Destination NAT Services Gateway)....654
(IDP Policy)....654
(LDAP)....31
(RADIUS)....31
(Security Policies)....655
(Source NAT Services Gateway)....655
source-address-filter statement....153
source-except statement....656
source-filtering statement....154
source-interface statement....656
source-ip-based statement....657
source-nat statement: (Source NAT Services Gateway)....658
source-port statement....49, 659
source-threshold statement....660
space-time-block-coding statement
WLAN....921
spam-action....660
spi statement....661
sql statement....662
ssh-known-hosts statement....663
ssid statement
WLAN....921
ssl-inspection statement....664
start-date statement....229
start-log statement....664
start-time statement....230, 665
static statement....665
WLAN....921
static-mac statement....57
static-wep statement
WLAN....922

station statement....837
station-mac-filter statement
WLAN....923
station-queues statement
WLAN....924
station-template statement....838
station-type statement....838
stop-date statement....231
stop-time statement....232
strict-syn-check statement....666
success statement....32
sunday statement....233
sunrpc statement....667
support, technical *See* technical support
suppression statement....668
surf-control-integrated....669
survivable-call-service statement....839
syn-ack-ack-proxy statement....670
syn-fin statement....670
syn-flood statement....671
syn-flood-protection-mode statement....672
syn-frag statement....672
syntax conventions....xli
System Configuration Statement Hierarchy....863
system-generated-certificate statement....878
system-services statement....673
(Interface Host-Inbound Traffic)....674
(Zone Host-Inbound Traffic)....676

T

t1-interval statement....677
t4-interval statement....678
talk statement....679
target statement....680
tcp statement....681
(Protocol Binding Custom Attack)....681
(Security Screen)....682
(Signature Attack)....683
tcp-flags statement....685
tcp-initial-timeout statement....686
tcp-mss statement....687
tcp-no-flag statement....688
tcp-rst statement....688
tcp-session statement....689
tdm-interface (direct-inward-line)....840
tdm-interface statement (station-type)....840
technical support
contacting JTAC....xlii
telemetries statement....163
telnet statement....32
term statement....50, 842
terminal statement....689
test statement....690
test-only-mode statement....843
tftp statement....691
then statement....692
(Destination NAT Services Gateway)....692
(IDP Policy)....693, 694
(Security Policies)....695
(Source NAT Services gateway)....696
then statement (route-policy)....842
threshold statement....74, 697
thursday statement....234
time-binding statement....697
time-binding-count statement....698
time-binding-period statement....699
timeout (antivirus fallback-options)....702
timeout (antivirus scan-options)....703
timeout (antivirus trickling)....703
timeout (utm)....702
timeout (web-filtering fallback-settings)....704
timeout (web-filtering surf-control-integrated
cache)....704
timeout (web-filtering websense-redirect profile)....705
timeout statement....33, 700, 844
(IDP Policy)....700
(LDAP Server)....33
(RADIUS Server)....33
(Security Screen)....701
timeout-action statement....845
timout (gtp)....700
to statement....705
to-zone statement....706
too-many-requests....707
too-many-requests (antivirus fallback-options)....707
too-many-requests (web-filtering
fallback-settings)....708
tos statement....709
total-length statement....710
traceoptions statement....34, 75, 711, 846, 879
(firewall-authentication)....712
(Flow)....714
(General Authentication Service)....880
(GTP)....716
(H.323 ALG)....713
(IDP)....717
(IKE)....719
(IPsec)....720
(MGCP ALG)....721
(NAT Services Gateway)....722
(PKI)....725
(Policies)....727
(SCCP ALG)....729
(Screen)....730
(Security)....732
(SIP ALG)....734
(WAN Acceleration)....882
ES-IS....198
tracing flags
ES-IS....198
traffic-options....735

transaction-timeout statement....735
transmit-opportunity-limit statement
WLAN....925
transmit-power statement
WLAN....925
transmit-rate-sets statement
WLAN....926
transport statement....847
trickling....736
trigger statement....96
trunk statement....848
trunk-group statement....849, 850
trusted-ca statement....736
ttl statement....737
tuesday statement....235
tunable-name statement....737
tunable-value statement....738
tunnel statement....738
tunnel-queuing statement....76
type (antivirus fallback-block)....740
type (antivirus notification-options
virus-detection)....741
type (content-filtering notification-options)....741
type (utm)....740
type statement....739
(Dynamic Attack Group)....739
(ICMP Headers in Signature Attack)....739

U

udp statement....742
(Protocol Binding Custom Attack)....742
(Security Screen)....743
(Signature Attack)....744
unified-access-control statement....852
unknown-message statement....745
(H.323.ALG)....745
(MGCP ALG)....746
(SCCP ALG)....747
(SIP ALG)....748
untagged-vlan statement
WLAN....926
update-server statement....154
upload-profile....749
upload-profile (ftp antivirus utm-profile)....749
upload-profile (ftp content-filtering utm-profile)....749
urgent-pointer statement....750
url (antivirus)....751
url (juniper-express-engine)....751
url (kaspersky-lab-engine)....751
url statement....750
url-blacklist....752
url-pattern....752
url-whitelist....753
url-whitelist (antivirus)....753
url-whitelist (web-filtering)....753
user statement....754
user-at-hostname statement....754
utm statement....755
utm-policy....760
uuid statement....51

V

value-hit-rate-threshold statement....761
vendor-id statement....155
video-queue statement
WLAN....927
virtual-access-point statement
WLAN....928
virtual-channel-group statement....98
virtual-channel-groups statement....99
virtual-channels statement....97
virus-detection....762
vlan statement
WLAN....929
vlan-id statement....57
vlan-id-list statement....58
vlan-tagging statement....156
voice-activity-detection statement....853
voice-queue statement
WLAN....930
voicemail statement....854
vpn statement....113, 763
vpn-monitor statement....764
vpn-monitor-options statement....765

W

wan-acceleration statement....883
web-authentication statement....35, 156, 766
web-redirect statement....767
wednesday statement....236
weight statement....77
wildcard statement....768
window-scale statement....768
window-size statement....769
winnuke statement....769
WLAN Configuration Statement Hierarchy....885
wpa-enterprise statement
WLAN....931
wpa-personal statement
WLAN....932

X

xauth statement....770

Z

zone statement....855
zones statement....771