JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Security Policies User Guide for Security Devices

Published
2020-03-29

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

Junos® OS Security Policies User Guide for Security Devices
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | xv

Documentation and Release Notes | **xv**

Using the Examples in This Manual | **xv**

- Merging a Full Example | **xvi**
- Merging a Snippet | **xvii**

Documentation Conventions | **xvii**

Documentation Feedback | **xx**

Requesting Technical Support | **xx**

- Self-Help Online Tools and Resources | **xxi**
- Creating a Service Request with JTAC | **xxi**

1 **Overview**

Security Basics Overview | 23

Security Policies Overview | 23

2 **Security Zones**

Security Zones | 27

- Security Zones Overview | **27**
  - Understanding Security Zone Interfaces | **28**
  - Understanding Functional Zones | **28**
  - Understanding Security Zones | **29**
- Example: Creating Security Zones | **29**
- Supported System Services for Host Inbound Traffic | **32**
- Understanding How to Control Inbound Traffic Based on Traffic Types | **33**
- Example: Controlling Inbound Traffic Based on Traffic Types | **34**
- Understanding How to Control Inbound Traffic Based on Protocols | **37**
- Example: Controlling Inbound Traffic Based on Protocols | **38**
- Example: Configuring the TCP-Reset Parameter | **40**

3 Address Books and Address Sets

Address Books and Address Sets | 44

Understanding Address Books | 44

Predefined Addresses | 45

Network Prefixes in Address Books | 45

Wildcard Addresses in Address Books | 45

DNS Names in Address Books | 46

Understanding Global Address Books | 46

Understanding Address Sets | 47

Limitations of Addresses and Address Sets in a Security Policy | 47

Configuring Addresses and Address Sets | 48

Addresses and Address Sets | 48

Address Books and Security Zones | 49

Address Books and Security Policies | 50

Address Books and NAT | 52

Example: Configuring Address Books and Address Sets | 53

Excluding Addresses from Policies | 60

Example: Excluding Addresses from Policies | 61

4 Security Policy Applications and Application Sets

Security Policy Applications and Application Sets | 69

Security Policy Applications Overview | 69

Security Policy Application Sets Overview | 70

Example: Configuring Security Policy Applications and Application Sets | 71

Understanding Policy Application Timeout Configuration and Lookup | 72

Understanding Policy Application Timeouts Contingencies | 73

Example: Setting a Policy Application Timeout | 74

Predefined Policy Applications | 75

Understanding Internet-Related Predefined Policy Applications | 76

Understanding Microsoft Predefined Policy Applications | 78

Understanding Dynamic Routing Protocols Predefined Policy Applications | 79

Understanding Streaming Video Predefined Policy Applications | 79

Understanding Sun RPC Predefined Policy Applications | 80

Understanding Security and Tunnel Predefined Policy Applications | 81

Understanding IP-Related Predefined Policy Applications | 82

Understanding Instant Messaging Predefined Policy Applications | 82

Understanding Management Predefined Policy Applications | 83

Understanding Mail Predefined Policy Applications | 85

Understanding UNIX Predefined Policy Applications | 85

Understanding Miscellaneous Predefined Policy Applications | 86

Understanding ICMP Predefined Policy Applications | 87

Default Behavior of ICMP Unreachable Errors | 92

Example: Defining a Custom ICMP Application | 93

Custom Policy Applications | 96

Understanding Custom Policy Applications | 96

Custom Application Mappings | 96

Example: Adding and Modifying Custom Policy Applications | 97

Example: Configuring Custom Policy Application Term Options | 100

5 **Security Policies**

Configuring Security Policies | 105

Understanding Security Policy Elements | 105

Understanding Security Policy Rules | 106

Understanding Wildcard Addresses | 109

Understanding Security Policies for Self Traffic | 110

Security Policies Configuration Overview | 111

Best Practices for Defining Policies on SRX Series Devices | 111

Configuring Policies Using the Firewall Wizard | 115

Example: Configuring a Security Policy to Permit or Deny All Traffic | 115

Example: Configuring a Security Policy to Permit or Deny Selected Traffic | 120

Example: Configuring a Security Policy to Permit or Deny Wildcard Address Traffic | 125

Example: Configuring a Security Policy to Redirect Traffic Logs to an External System Log Server | 129

TAP Mode for Security Zones and Policies | 133

Understanding TAP Mode Support for Security Zones and Policies | 133

Example: Configuring Security Zones and Policies in TAP mode | 134

Dynamic Address Groups in Security Policies | **138**

Bundle Feeds | **140**

Feed Server Support for SRX Series Devices | **143**

Unified Security Policies | 145

Unified Policies Overview | **145**

Benefits | **146**

Unified Policies Configuration Overview | **146**

Dynamic Application Configuration Options | **147**

Default Ports and Protocols as Application Matching Criteria | **147**

Default Policy Actions Prior to Dynamic Application Identification | **148**

Global Policy Utilization with Unified Policies | **149**

Unified Policy Actions | **149**

Redirect Profile for Reject Action | **149**

SSL Proxy Profile for Reject Action | **150**

Match Criteria and Rules for Unified Policies | **151**

Limitations to Configuring Unified Policies | **153**

Example: Configure a Unified Policy Using a Redirect Message Profile | **154**

Configure a URL Category with Unified Policies | **160**

Understanding URL Category with Unified Policies | **160**

Example: Configuring a Unified Policy Using URL Category | **160**

Configure Applications in Unified Policies | **165**

Applications in Unified Policies | **165**

Example: Configure a Unified Policy Using Dynamic Applications | **166**

Configure Micro-Applications in Unified Policies | **170**

Limit the Number of Policy Lookups | **170**

Configure Micro-Applications | **171**

Global Security Policies | 172

Global Policy Overview | **172**

Example: Configuring a Global Policy with No Zone Restrictions | **175**

Example: Configuring a Global Policy with Multiple Zones | **179**

User Role Firewall Security Policies | 182

Understanding User Role Firewalls | **183**

User Role Retrieval and the Policy Lookup Process | **183**

Understanding the User Identification Table | **186**

Local Authentication Table | **187**

UAC Authentication Table | **189**

Firewall Authentication Table | **190**

Policy Provisioning With Users and Roles | **191**

Obtaining Username and Role Information Through Firewall Authentication | **192**

Configuring a User Role Firewall For Captive Portal Redirection | **193**

Example: Configuring a User Role Firewall on an SRX Series Device | **195**

Configuring Resource Policies Using UAC | **203**

Reordering Security Policies | 206

Understanding Security Policy Ordering | **206**

Example: Reordering Security Policies | **208**

Scheduling Security Policies | 209

Security Policy Schedulers Overview | **210**

Example: Configuring Schedulers for a Daily Schedule Excluding One Day | **211**

Verifying Scheduled Policies | **214**

Configuring Security Policies for a VRF Routing Instance | 215

Overview | **216**

Controlling Traffic in SD-WAN Architecture | **216**

Understanding Security Policy Rules | **217**

| **217**

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network | **218**

Example: Configuring a Security Policy to Permit VRF-Based Traffic from an IP Network to an MPLS Network | **224**

Example: Configuring a Security Policy to Permit VRF-Based Traffic from an MPLS Network to an MPLS Network over GRE without NAT | **229**

Example: Configuring Security Policies Using VRF Routing Instances in an MPLS Network | **235**

Configuring Security Policies Using VRF Group | 246

Overview | **247**

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network using Source VRF Group | **248**

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from an IP Network to MPLS Network using Destination VRF Group | **252**

Managing Overlapping VPN using VRF group | **257**

Monitoring and Troubleshooting Security Policies | 258

Understanding Security Alarms | **258**

Example: Generating a Security Alarm in Response to Policy Violations | **259**

Matching Security Policies | **262**

Tracking Policy Hit Counts | **264**

Checking Memory Usage on SRX Series Devices | **264**

Monitoring Security Policy Statistics | **266**

Verifying Shadow Policies | **266**

Verifying All Shadow Policies | **267**

Verifying a Policy Shadows One or More Policies | **267**

Verifying a Policy Is Shadowed by One or More Policies | **268**

Troubleshooting Security Policies | **269**

Synchronizing Policies Between Routing Engine and Packet Forwarding Engine | **269**

Checking a Security Policy Commit Failure | **270**

Verifying a Security Policy Commit | **270**

Debugging Policy Lookup | **271**

High Availability (HA) Synchronization of Address Name Resolving Cache | **271**

6 **Configuration Statements**

address (Security Address Book) | 278

address-book | 281

address-set | 283

alarms (Security) | 284

alarm-threshold | 286

alarm-without-drop | 287

application (Applications) | 288

application (Security Alarms) | 292

application (Security Policies) | 293

application-protocol (Applications) | 295

application-services (Security Policies) | 297

application-tracking (Security Zones) | 299

application-traffic-control (Application Services) | 300

attach | 301

audible (Security Alarms) | 302

authentication (Security Alarms) | 303

authentication-source (Security) | 304

captive-portal (Services UAC Policy) | 305

count (Security Policies) | 306

default-policy | 307

deny (Security Policies) | 308

description (Applications) | 309

description (Security Address Book) | 310

description (Security Zone) | 311

destination-address (Security Policies) | 312

destination-address (Security Policies Flag) | 313

destination-address-excluded | 314

destination-ip (Security Alarms) | 315

destination-port (Applications) | 317

dns-cache | 322

dns-proxy | 324

dynamic-application (Security) | 326

dynamic-application (Security Policies) | 328

dynamic-dns | 330

exclude (Schedulers) | 331

firewall-authentication (Security Policies) | 332

firewall-authentication (User Identification) | 334

forward-only (DNS) | 335

from-zone (Security Policies) | 336

from-zone (Security Policies Global) | 341

functional-zone | 342

global (Security Policies) | 344

host-inbound-traffic | 348

icmp-code (Applications) | 349

icmp-type (Applications) | 350

inactivity-timeout (Applications) | 351

interfaces (Security Zones) | 352

initial-tcp-mss | 353

ipsec-group-vpn (Security Policies) | 354

ipsec-vpn (Security Policies) | 355

local-authentication-table | 356

log (Security Policies) | 357

management (Security Zones) | 358

match (Security Policies) | 360

match (Security Policies Global) | 362

unified-policy max-lookups | 364

no-policy-cold-synchronization | 365

pair-policy | 366

pass-through | 367

permit (Security Policies) | 369

policies | 371

policy (Security Alarms) | 382

policy (Security Policies) | 384

policy-match | 388

policy-rematch | 390

policy-stats | 391

potential-violation | 392

pre-id-default-policy | 395

profile(dynamic-application) | 397

protocol (Applications) | 399

protocols (Security Zones Host Inbound Traffic) | 401

protocols (Security Zones Interfaces) | 403

range-address | 405

redirect-wx (Application Services) | 406

reject (Security) | 407

report-skip | 408

reverse-tcp-mss | 409

rpc-program-number (Applications) | 410

scheduler (Security Policies) | 411

scheduler-name | 413

schedulers (Security Policies) | 414

screen (Security Zones) | 415

secure-domains | 416

secure-neighbor-discovery | 417

security-zone | 418

sequence-check-required | 420

services-offload (Security) | 421

session-close | 422

session-init | 423

simple-mail-client-service | 424

source-address (Security Policies) | 425

source-address-excluded | 426

source-identity | 427

source-ip (Security Alarms) | 429

source-port (Applications) | 430

ssl-proxy (Application Services) | 431

ssl-termination-profile | 432

start-date | 433

start-time (Schedulers) | 434

stop-date | 435

stop-time | 436

syn-check-required | 437

system-services (Security Zones Host Inbound Traffic) | 438

system-services (Security Zones Interfaces) | 441

tcp-options (Security Policies) | 443

tcp-rst | 445

term (Applications) | 446

then (Security Policies) | 447

to-zone (Security Policies) | 450

to-zone (Security Policies Global) | 454

traceoptions (dynamic-application) | 455

traceoptions (Security Policies) | 457

traceoptions (Security User Identification) | 459

traceoptions (System Services DNS) | 461

tunnel (Security Policies) | 464

uac-policy (Application Services) | 465

unified-access-control (Security) | 466

unified-policy-explicit-match | 467

user-firewall | 468

user-identification | 470

utm-policy | 472

uuid (Applications) | 474

vrrp | 475

web-authentication | 476

web-redirect | 477

zones | 478

7 Operational Commands

clear security alarms | 483

clear security policies hit-count | 487

clear security policies statistics | 488

clear system services dns dns-proxy | 489

request security policies check | 490

request security policies resync | 493

request security user-identification local-authorization-table add | 495

request security user-identification local-authentication-table delete | 497

show security alarms | 499

show security firewall-authentication users address | 505

show security firewall-authentication users auth-type | 509

show security flow session application | 512

show security match-policies | 517

show security policies | 524

show security policies checksum | 541

show security policies hit-count | 544

show security policies information | 548

show security policies unknown-source-identity | 554

show security policies zone-context | 556

show security policy-report | 559

show security shadow-policies | 563

show security user-identification local-authentication-table | 566

show security user-identification role-provision all | 569

show security user-identification source-identity-provision all | 571

show security user-identification user-provision all | 573

show security zones | 575

show security zones type | 583

show system services dns dns-proxy | 587

show system services dynamic-dns | 590

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xv
- Using the Examples in This Manual | xv
- Documentation Conventions | xvii
- Documentation Feedback | xx
- Requesting Technical Support | xx

Use this guide to configure security zones, address books and address sets, security policy applications and application sets, and security policies in Junos OS on the SRX Series devices.

Documentation and 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 https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
       scripts {
           commit {
               file ex-script.xsl;
           }
       }
   }
   interfaces {
       fxp0 {
           disable;
           unit 0 {
               family inet {
                   address 10.0.0.1/24;
               }
           }
       }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; 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)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (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)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies 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.	
GUI Conventions		

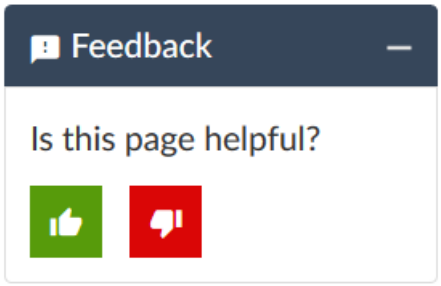
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents 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 menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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, see https://support.juniper.net/support/requesting-support/.

1

CHAPTER

Overview

Security Basics Overview | 23

Security Policies Overview | 23

Security Basics Overview

This guide provides information about the security basics used to configure features for security devices.

- A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. With many types of Juniper Networks devices, you can define multiple security zones, the exact number of which you determine based on your network needs.
- An address book is a collection of addresses and address sets. Junos OS allows you to configure multiple address books. Address books are like components, or building blocks, that are referenced in other configurations such as security policies or NAT. You can add addresses to address books or use the predefined addresses available to each address book by default.
- An application set is a group of applications. Junos OS simplifies the process by allowing you to manage a small number of application sets, rather than a large number of individual application entries. The application (or application set) is referred to by security policies as match criteria for packets initiating sessions.
- A security policy is a stateful firewall policy that provides a set of tools to network administrators, enabling them to implement network security for their organizations. Security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall.

RELATED DOCUMENTATION

> *Getting Started Guide for Junos OS*

Security Policies Overview

To secure their business, organizations must control access to their LAN and their resources. Security policies are commonly used for this purpose. Secure access is required both within the company across the LAN and in its interactions with external networks such as the Internet. Junos OS provides powerful network security features through its stateful firewall, application firewall, and user identity firewall. All three types of firewall enforcement are implemented through security policies. The stateful firewall policy syntax is widened to include additional tuples for the application firewall and the user identity firewall.

In a Junos OS stateful firewall, the security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the

firewall. From the perspective of security policies, the traffic enters one security zone and exits another security zone. This combination of a *from-zone* and *to-zone* is called a *context*. Each context contains an *ordered list* of policies. Each policy is processed in the order that it is defined within a context.

A security policy, which can be configured from the user interface, controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specified IP sources to specified IP destinations at scheduled times.

Policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another. You decide which users and what data can enter and exit, and when and where they can go.

> **NOTE:** For an SRX Series device that supports virtual systems, policies set in the root system do not affect policies set in virtual systems.

An SRX Series device secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another.

Logging capability can also be enabled with security policies during session initialization (**session-init**) or session close (**session-close**) stage.

- To view logs from denied connections, enable log on **session-init**.
- To log sessions after their conclusion/tear-down, enable log on **session-close**.

> **NOTE:** Session log is enabled at real time in the flow code which impacts the user performance. If both **session-close** and **session-init** are enabled, performance is further degraded as compared to enabling **session-init** only.

For SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices, a factory-default security policy is provided that:

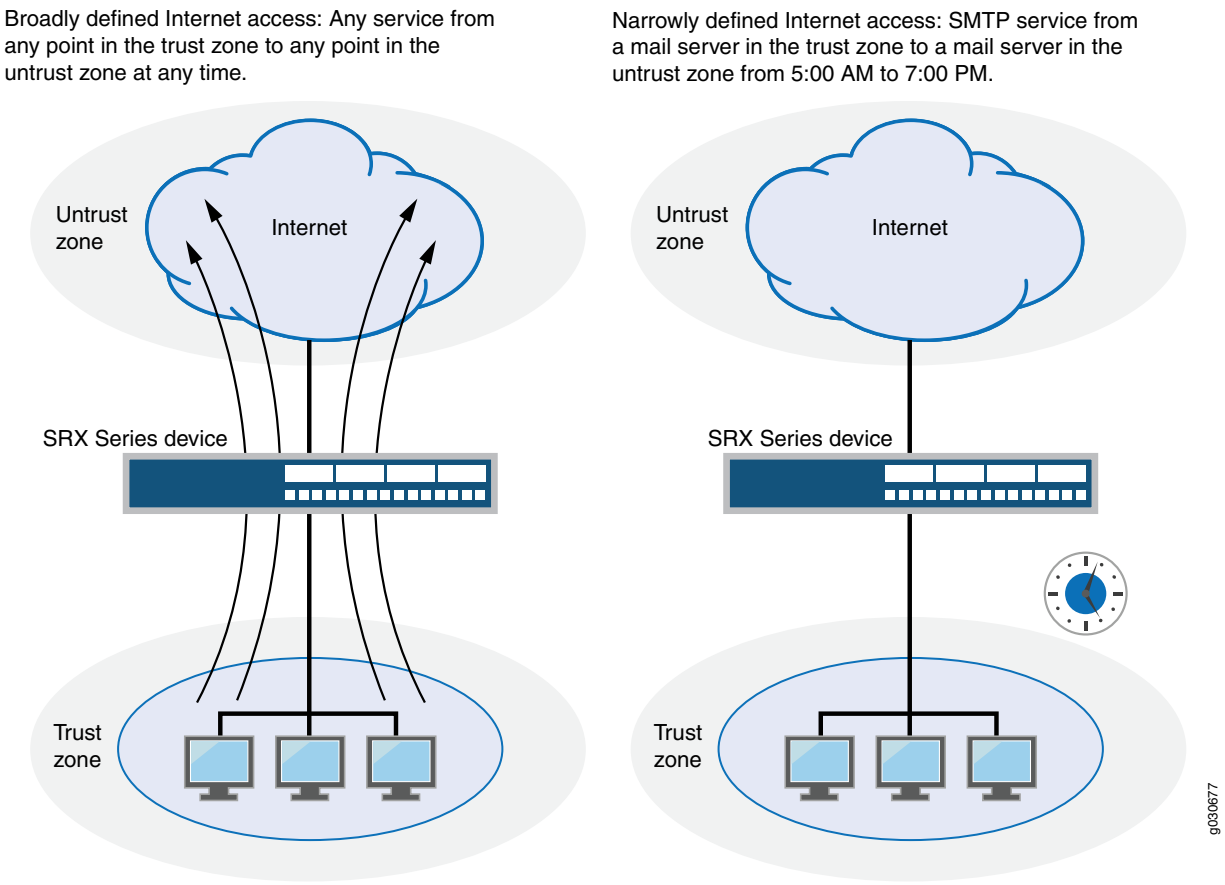
- Allows all traffic from the trust zone to the untrust zone.
- Allows all traffic between trusted zones, that is from the trust zone to intrazone trusted zones.
- Denies all traffic from the untrust zone to the trust zone.

Through the creation of policies, you can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations at scheduled times.

At the broadest level, you can allow all kinds of traffic from any source in one zone to any destination in all other zones without any scheduling restrictions. At the narrowest level, you can create a policy that

allows only one kind of traffic between a specified host in one zone and another specified host in another zone during a scheduled interval of time. See Figure 1 on page 25.

Figure 1: Security Policy



Every time a packet attempts to pass from one zone to another or between two interfaces bound to the same zone, the device checks for a policy that permits such traffic (see "Understanding Security Zones" on page 29 and "Example: Configuring Security Policy Applications and Application Sets" on page 71). To allow traffic to pass from one security zone to another—for example, from zone A to zone B—you must configure a policy that permits zone A to send traffic to zone B. To allow traffic to flow the other way, you must configure another policy permitting traffic from zone B to zone A.

To allow data traffic to pass between zones, you must configure firewall policies.

RELATED DOCUMENTATION

2
CHAPTER

Security Zones

Security Zones | 27

Security Zones

IN THIS SECTION

- Security Zones Overview | 27
- Example: Creating Security Zones | 29
- Supported System Services for Host Inbound Traffic | 32
- Understanding How to Control Inbound Traffic Based on Traffic Types | 33
- Example: Controlling Inbound Traffic Based on Traffic Types | 34
- Understanding How to Control Inbound Traffic Based on Protocols | 37
- Example: Controlling Inbound Traffic Based on Protocols | 38
- Example: Configuring the TCP-Reset Parameter | 40

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. You can define multiple security zones, the exact number of which you determine based on your network needs.

Security Zones Overview

IN THIS SECTION

- Understanding Security Zone Interfaces | 28
- Understanding Functional Zones | 28
- Understanding Security Zones | 29

Interfaces act as a doorway through which traffic enters and exits a Juniper Networks device. Many interfaces can share exactly the same security requirements; however, different interfaces can also have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single security zone.

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies.

Security zones are logical entities to which one or more interfaces are bound. With many types of Juniper Networks devices, you can define multiple security zones, the exact number of which you determine based on your network needs.

On a single device, you can configure multiple security zones, dividing the network into segments to which you can apply various security options to satisfy the needs of each segment. At a minimum, you must define two security zones, basically to protect one area of the network from the other. On some security platforms, you can define many security zones, bringing finer granularity to your network security design—and without deploying multiple security appliances to do so.

From the perspective of security policies, traffic enters into one security zone and goes out on another security zone. This combination of a **from-zone** and a **to-zone** is defined as a *context*. Each context contains an ordered list of policies. For more information on policies, see "Security Policies Overview" on page 23.

This topic includes the following sections:

Understanding Security Zone Interfaces

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone.

Through the policies you define, you can permit traffic between zones to flow in one direction or in both. With the routes that you define, you specify the interfaces that traffic from one zone to another must use. Because you can bind multiple interfaces to a zone, the routes you chart are important for directing traffic to the interfaces of your choice.

An interface can be configured with an IPv4 address, IPv6 address, or both.

Understanding Functional Zones

A functional zone is used for special purposes, like management interfaces. Currently, only the management (MGT) zone is supported. Management zones have the following properties:

- Management zones host management interfaces.
- Traffic entering management zones does not match policies; therefore, traffic cannot transit out of any other interface if it was received in the management interface.
- Management zones can only be used for dedicated management interfaces.

Understanding Security Zones

Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them.

Security zones have the following properties:

- Policies—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall. For more information, see "Security Policies Overview" on page 23.
- Screens—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful. For more information, see *Reconnaissance Deterrence Overview*.
- Address books—IP addresses and address sets that make up an address book to identify its members so that you can apply policies to them. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and Domain Name System (DNS) names. For more information, see "Example: Configuring Address Books and Address Sets" on page 53.
- TCP-RST—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.
- Interfaces—List of interfaces in the zone.

Security zones have the following preconfigured zone:

- Trust zone—Available only in the factory configuration and is used for initial connection to the device. After you commit a configuration, the trust zone can be overridden.

Example: Creating Security Zones

IN THIS SECTION

- Requirements | 30
- Overview | 30
- Configuration | 30
- Verification | 32

This example shows how to configure zones and assign interfaces to them. When you configure a security zone, you can specify many of its parameters at the same time.

Requirements

Before you begin, configure network interfaces. See the *Interfaces User Guide for Security Devices*.

Overview

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone.

> **NOTE:** By default, interfaces are in the null zone. The interfaces will not pass traffic until they have been assigned to a zone.

> **NOTE:** You can configure 2000 interfaces within a security zone on SRX3400, SRX3600, SRX4600, SRX5400, SRX5600, or SRX5800 devices, depending on the Junos OS release in your installation.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet address 203.0.113.1/24
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1::1/64
set security zones security-zone ABC interfaces ge-0/0/1.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To create zones and assign interfaces to them:

1. Configure an Ethernet interface and assign an IPv4 address to it.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 203.0.113.1/24
```

2. Configure an Ethernet interface and assign an IPv6 address to it.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8::1/32
```

3. Configure a security zone and assign it to an Ethernet interface.

```
[edit]
user@host# set security zones security-zone ABC interfaces ge-0/0/1.0
```

Results

From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC** and **show interfaces ge-0/0/1** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
```

```
user@host# show security zones security-zone ABC
```

```
...
    interfaces {
        ge-0/0/1.0 {
            ...
        }
    }
```

```
[edit]
```

```
user@host# show interfaces ge-0/0/1
```

```
...
        unit 0 {
        family inet {
            address 203.0.113.1/24;
        }
```

```
        family inet6 {
            address 2001:db8:1::1/64;
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

From operational mode, enter the **show log messages** command and the **show log dcd** command.

Supported System Services for Host Inbound Traffic

This topic describes the supported system services for host inbound traffic on the specified zone or interface.

For example, suppose a user whose system was connected to interface **203.0.113.4** in zone **ABC** wanted to telnet into interface **198.51.100.4** in zone **ABC**. For this action to be allowed, the Telnet application must be configured as an allowed inbound service on both interfaces and a policy must permit the traffic transmission.

See the *Options* section in **system-services (Security Zones Host Inbound Traffic)** to view the system services that can be used for host inbound traffic.

> **NOTE:** On SRX Series Services Gateways, the **xnm-clear-text** field is enabled in the factory-default configuration. This setting enables incoming Junos XML protocol traffic in the trust zone for the device when the device is operating with factory-default settings. We recommend that you replace the factory-default settings with a user-defined configuration that provides additional security once the box is configured. You must delete the **xnm-clear-text** field manually by using the CLI command **delete system services xnm-clear-text**.

See the *Options* section in **protocols (Security Zones Interfaces)** to view the supported protocols that can be used for host inbound traffic.

NOTE: All services (except DHCP and BOOTP) can be configured either per zone or per interface. A DHCP server is configured only per interface because the incoming interface must be known by the server to be able to send out DHCP replies.

NOTE: You do not need to configure Neighbor Discovery Protocol (NDP) on host-inbound traffic, because the NDP is enabled by default.

Configuration option for IPv6 Neighbor Discovery Protocol (NDP) is available. The configuration option is **set protocol neighbor-discovery onlink-subnet-only** command. This option will prevent the device from responding to a Neighbor Solicitation (NS) from a prefix which was not included as one of the device interface prefixes.

NOTE: The Routing Engine needs to be rebooted after setting this option to remove any possibility of a previous IPv6 entry from remaining in the forwarding-table.

Understanding How to Control Inbound Traffic Based on Traffic Types

This topic describes how to configure zones to specify the kinds of traffic that can reach the device from systems that are directly connected to its interfaces.

Note the following:

- You can configure these parameters at the zone level, in which case they affect all interfaces of the zone, or at the interface level. (Interface configuration overrides that of the zone.)
- You must enable all expected host-inbound traffic. Inbound traffic destined to this device is dropped by default.
- You can also configure a zone's interfaces to allow for use by dynamic routing protocols.

This feature allows you to protect the device against attacks launched from systems that are directly or indirectly connected to any of its interfaces. It also enables you to selectively configure the device so that administrators can manage it using certain applications on certain interfaces. You can prohibit use of other applications on the same or different interfaces of a zone. For example, most likely you would want to ensure that outsiders not use the Telnet application from the Internet to log in to the device because you would not want them connecting to your system.

Example: Controlling Inbound Traffic Based on Traffic Types

IN THIS SECTION

- Requirements | 34
- Overview | 34
- Configuration | 34
- Verification | 37

This example shows how to configure inbound traffic based on traffic types.

Requirements

Before you begin:

- Configure network interfaces. See *Interfaces User Guide for Security Devices*.
- Understand Inbound traffic types. See "Understanding How to Control Inbound Traffic Based on Traffic Types" on page 33.

Overview

By allowing system services to run, you can configure zones to specify different types of traffic that can reach the device from systems that are directly connected to its interfaces. You can configure the different system services at the zone level, in which case they affect all interfaces of the zone, or at the interface level. (Interface configuration overrides that of the zone.)

You must enable all expected host-inbound traffic. Inbound traffic from devices directly connected to the device's interfaces is dropped by default.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone ABC host-inbound-traffic system-services all
```

```
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic system-services telnet
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic system-services ftp
set security zones security-zone ABC interfaces ge-0/0/1.3 host-inbound-traffic system-services snmp
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic system-services all
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic system-services ftp except
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic system-services http except
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure inbound traffic based on traffic types:

1. Configure a security zone.

```
[edit]
user@host# edit security zones security-zone ABC
```

2. Configure the security zone to support inbound traffic for all system services.

```
[edit security zones security-zone ABC]
user@host# set host-inbound-traffic system-services all
```

3. Configure the Telnet, FTP, and SNMP system services at the interface level (not the zone level) for the first interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services telnet
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services ftp
user@host# set interfaces ge-0/0/1.3 host-inbound-traffic system-services snmp
```

4. Configure the security zone to support inbound traffic for all system services for a second interface.

```
[edit security zones security-zone ABC]
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services all
```

5. Exclude the FTP and HTTP system services from the second interface.

```
[edit security zones security-zone ABC]
```

```
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services ftp except
user@host# set interfaces ge-0/0/1.0 host-inbound-traffic system-services http except
```

Results

From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC**. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
```

```
user@host# show security zones security-zone ABC
```

```
host-inbound-traffic {
    system-services {
        all;
    }
}
    interfaces {
    ge-0/0/1.3 {
        host-inbound-traffic {
            system-services {
                ftp;
                telnet;
                snmp;
            }
        }
    }
    ge-0/0/1.0 {
        host-inbound-traffic {
            system-services {
                all;
                ftp {
                    except;
                }
                http {
                    except;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

From operational mode, enter the **show log messages** command and the **show log dcd** command.

Understanding How to Control Inbound Traffic Based on Protocols

This topic describes the inbound system protocols on the specified zone or interface.

Any host-inbound traffic that corresponds to a protocol listed under the host-inbound traffic option is allowed. For example, if anywhere in the configuration, you map a protocol to a port number other than the default, you can specify the protocol in the host-inbound traffic option, and the new port number will be used. Table 3 on page 37 lists the supported protocols. A value of **all** indicates that traffic from all of the following protocols is allowed inbound on the specified interfaces (of the zone, or a single specified interface).

Table 3: Supported Inbound System Protocols

Supported System Services			
all	igmp	pim	sap
bfd	ldp	rip	vrrp
bgp	msdp	ripng	nhrp
router-discovery	dvmrp	ospf	rsvp
pgm	ospf3		

NOTE: If DVMRP or PIM is enabled for an interface, IGMP and MLD host-inbound traffic is enabled automatically. Because IS-IS uses OSI addressing and should not generate any IP traffic, there is no host-inbound traffic option for the IS-IS protocol.

> **NOTE:** You do not need to configure Neighbor Discovery Protocol (NDP) on host-inbound traffic, because the NDP is enabled by default.

Configuration option for IPv6 Neighbor Discovery Protocol (NDP) is available. The configuration option is **set protocol neighbor-discovery onlink-subnet-only** command. This option will prevent the device from responding to a Neighbor Solicitation (NS) from a prefix which was not included as one of the device interface prefixes.

> **NOTE:** The Routing Engine needs to be rebooted after setting this option to remove any possibility of a previous IPv6 entry remaining in the forwarding-table.

Example: Controlling Inbound Traffic Based on Protocols

IN THIS SECTION

- Requirements | 38
- Overview | 39
- Configuration | 39
- Verification | 40

This example shows how to enable inbound traffic for an interface.

Requirements

Before you begin:

- Configure security zones. See “Example: Creating Security Zones” on page 29.
- Configure network interfaces. See the *Interfaces User Guide for Security Devices*.

Overview

Any host-inbound traffic that corresponds to a protocol listed under the host-inbound traffic option is allowed. For example, if anywhere in the configuration you map a protocol to a port number other than the default, you can specify the protocol in the host-inbound traffic option, and the new port number will be used.

A value of **all** indicates that traffic from all of the protocols is allowed inbound on the specified interfaces (of the zone, or a single specified interface).

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf
set security zones security-zone ABC interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf3
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure inbound traffic based on protocols:

1. Configure a security zone.

   ```
   [edit]
   user@host# edit security zones security-zone ABC
   ```

2. Configure the security zone to support inbound traffic based on the ospf protocol for an interface.

   ```
   [edit security zones security-zone ABC]
   user@host# set interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf
   ```

3. Configure the security zone to support inbound traffic based on the ospf3 protocol for an interface.

   ```
   [edit security zones security-zone ABC]
   user@host# set interfaces ge-0/0/1.0 host-inbound-traffic protocols ospf3
   ```

Results

From configuration mode, confirm your configuration by entering the **show security zones security-zone ABC**. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
```

```
user@host# show security zones security-zone ABC
```

```
interfaces {
    ge-0/0/1.0 {
        host-inbound-traffic {
            protocols {
                ospf;
                ospf3;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

From operational mode, enter the **show log messages** command and the **show log dcd** command.

Example: Configuring the TCP-Reset Parameter

IN THIS SECTION

- Requirements | 41
- Overview | 41

Configuration | 41
Verification | 42

This example shows how to configure the TCP-Reset parameter for a zone.

Requirements

Before you begin, configure security zones. See “Example: Creating Security Zones” on page 29.

Overview

When the TCP-Reset parameter feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYN flag set.

Configuration

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure the TCP-Reset parameter for a zone:

1. Configure a security zone.

```
[edit]
user@host# edit security zones security-zone ABC
```

2. Configure the TCP-Reset parameter for the zone.

```
[edit security zones security-zone ABC]
user@host# set tcp-rst
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security zones** command.

RELATED DOCUMENTATION

Configuring Security Policies | **105**

3

CHAPTER

Address Books and Address Sets

Address Books and Address Sets | 44

Address Books and Address Sets

IN THIS SECTION

- Understanding Address Books | 44
- Understanding Global Address Books | 46
- Understanding Address Sets | 47
- Limitations of Addresses and Address Sets in a Security Policy | 47
- Configuring Addresses and Address Sets | 48
- Example: Configuring Address Books and Address Sets | 53
- Excluding Addresses from Policies | 60
- Example: Excluding Addresses from Policies | 61

An address book is a collection of addresses and address sets. Address books are like components or building blocks, that are referenced in other configurations such as security policies, security zones, and NAT. You can add addresses to address books or use the predefined addresses available to each address book by default.

Address sets are groups of addresses used to manage large address books. Using address sets, you can organize addresses in logical groups and use them to easily configure other features, such as policies and NAT rules.

Understanding Address Books

IN THIS SECTION

- Predefined Addresses | 45
- Network Prefixes in Address Books | 45
- Wildcard Addresses in Address Books | 45
- DNS Names in Address Books | 46

An address book is a collection of addresses and address sets. Junos OS allows you to configure multiple address books. Address books are like components, or building blocks, that are referenced in other configurations such as security policies or NAT. You can add addresses to address books or use the predefined addresses available to each address book by default.

Address book entries include addresses of hosts and subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated. These addresses can be any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, or Domain Name System (DNS) names.

Predefined Addresses

You can either create addresses or use any of the following predefined addresses that are available by default:

- **Any**—This address matches any IP address. When this address is used as a source or destination address in a policy configuration, it matches the source and destination address of any packet.
- **Any-ipv4**—This address matches any IPv4 address.
- **Any-ipv6**—This address matches any IPv6 address.

Network Prefixes in Address Books

You can specify addresses as network prefixes in the prefix/length format. For example, 203.0.113.0/24 is an acceptable address book address because it translates to a network prefix. However, 203.0.113.4/24 is not acceptable for an address book because it exceeds the subnet length of 24 bits. Everything beyond the subnet length must be entered as 0 (zero). In special scenarios, you can enter a hostname because it can use the full 32-bit address length.

An IPv6 address prefix is a combination of an IPv6 prefix (address) and a prefix length. The prefix takes the form ipv6-prefix/prefix-length and represents a block of address space (or a network). The ipv6-prefix variable follows general IPv6 addressing rules. The /prefix-length variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. For example, 2001:db8::/32 is a possible IPv6 prefix. For more information on text representation of IPv6 addresses and address prefixes, see RFC 4291, *IP Version 6 Addressing Architecture.*

Wildcard Addresses in Address Books

Besides IP addresses and domain names, you can specify a wildcard address in an address book. A wildcard address is represented as A.B.C.D/wildcard-mask. The wildcard mask determines which of the bits in the IP address A.B.C.D should be ignored. For example, the source IP address 192.168.0.11/255.255.0.255 in a security policy implies that the security policy match criteria can discard the third octet in the IP address (symbolically represented as 192.168.*.11). Therefore, packets with source IP addresses such as

192.168.1.11 and 192.168.22.11 conform to the match criteria. However, packets with source IP addresses such as 192.168.0.1 and 192.168.1.21 do not satisfy the match criteria.

The wildcard address usage is not restricted to full octets only. You can configure any wildcard address. For example, the wildcard address 192.168. 7.1/255.255.7.255 implies that you need to ignore only the first 5 bits of the third octet of the wildcard address while making the policy match. If the wildcard address usage is restricted to full octets only, then wildcard masks with either 0 or 255 in each of the four octets only will be permitted.

DNS Names in Address Books

By default, you can resolve IPv4 and IPv6 addresses for a DNS. If IPv4 or IPv6 addresses are designated, you can resolve only those addresses by using the keywords ipv4-only and ipv6-only, respectively.

For SRX5400, SRX5600, and SRX5800 devices and vSRX instances, starting with Junos OS 15.1X49-D60, management traffic can originate from a specific source address for Domain Name System (DNS) names.

Consider the following when you configure the source address for DNS:

- Only one source address can be configured as the source address for each DNS server name.
- IPv6 source addresses are supported for IPv6 DNS servers, and only IPv4 addresses are supported for IPv4 servers. You cannot configure an IPv4 address for an IPv6 DNS server or an IPv6 address for an IPv4 DNS server.

To have all management traffic originate from a specific source address, configure the system name server and the source address. For example:

```
user@host# set system name-server5.0.0.1 source-address 4.0.0.3
```

Before you can use domain names for address entries, you must configure the security device for DNS services. For information about DNS, see *DNS Overview*.

Understanding Global Address Books

An address book called “global” is always present on your system. Similar to other address books, the global address book can include any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, or Domain Name System (DNS) names.

You can create addresses in the global address book or use the predefined addresses (any, any-ipv4, and any-ipv6). However, to use the addresses in the global address book, you do not need to attach the security zones to it. The global address book is available to all security zones that have no address books attached to them.

Global address books are used in the following cases:

- NAT configurations–NAT rules can use address objects only from the global address book. They cannot use addresses from zone-based address books.
- Global policies–Addresses used in a global policy must be defined in global address book. Global address book objects do not belong to any particular zone.

Understanding Address Sets

An address book can grow to contain large numbers of addresses and become difficult to manage. You can create groups of addresses called address sets to manage large address books. Using address sets, you can organize addresses in logical groups and use them to easily configure other features, such as policies and NAT rules.

The predefined address set, **any**, which contains both **any-ipv4** and **any-ipv6** addresses, is automatically created for each security zone.

You can create address sets with existing users, or create empty address sets and later fill them with users. When creating address sets, you can combine IPv4 and IPv6 addresses, but the addresses must be in the same security zone.

You can also create an address set within an address set. This allows you to apply policies more effectively. For example, if you want to apply a policy to two address sets, **set1** and **set2**, instead of using two statements, you can use just one statement to apply the policy to a new address set, **set3**, that includes address sets **set1** and **set2**.

When you add addresses to policies, sometimes the same subset of addresses can be present in multiple policies, making it difficult to manage how policies affect each address entry. Reference an address set entry in a policy like an individual address book entry to allow you to manage a small number of address sets, rather than manage a large number of individual address entries.

Limitations of Addresses and Address Sets in a Security Policy

On SRX Series devices, one policy can reference multiple address sets, multiple address entries, or both. One address set can reference a maximum of 1024 address entries and a maximum of 256 address sets. There is a limit to the number of address objects that a policy can reference; the maximum number of address objects per policy is 1024. Starting with Junos OS Release 12.3X48-D15 and Junos OS Release 17.3R1, the maximum number of policies per context for SRX3400 and SRX3600 devices increases from 10,240 to 40,000, and for SRX5400, SRX5600, and SRX5800 devices, from 10240 to 80,000.

Note that every IPv6 address entry is equal to 4 IPv4 address entries. For example, a policy configured for 1000 IPv4 address entries and 5 IPv6 address entries has 1020 address objects (1000 + [5 x4] = 1020), which is within the 1024 value, and can be committed. However, a policy configured for 1000 IPv4 address entries and 7 IPv6 address entries has 1028 address objects (1000 +[7 x 4] = 1028), which exceeds the 1024 value, cannot be committed, and consequently generates an error message.

Configuring Addresses and Address Sets

IN THIS SECTION

- Addresses and Address Sets | **48**
- Address Books and Security Zones | **49**
- Address Books and Security Policies | **50**
- Address Books and NAT | **52**

You can define addresses and address sets in an address book and then use them when configuring different features. You can also use predefined addresses **any**, **any-ipv4**, and **any-ipv6** that are available by default. However, you cannot add the predefined address **any** to an address book.

After address books and sets are configured, they are used in configuring different features, such as security policies, security zones, and NAT.

Addresses and Address Sets

You can define IPv4 addresses, IPv6 addresses, wildcard addresses, or Domain Name System (DNS) names as address entries in an address book.

The following sample address book called **book1** contains different types of addresses and address sets. Once defined, you can leverage these addresses and address sets when you configure security zones, policies, or NAT rules.

```
[edit security address-book book1]
user@host# set address a1 203.0.113.1
user@host# set address a2 203.0.113.4/30
user@host# set address a4 2001:db8::/32
user@host# set address a5 2001:db8:1::1/127
user@host# set address example dns-name www.example.com
```

```
user@host# set address-set set1 address a1
user@host# set address-set set1 address a2
user@host# set address-set set1 address a2
user@host# set address-set set2 address bbc
```

When defining addresses and address sets, follow these guidelines:

- Address sets can only contain address names that belong to the same security zone.
- Address names **any**, **any-ipv4** and **any-ipv6** are reserved; you cannot use them to create any addresses.
- Addresses and address sets in the same zone must have distinct names.
- Address names cannot be the same as address set names. For example, if you configure an address with the name **add1**, do not create the address set with the name **add1**.
- When deleting an individual address book entry from the address book, you must remove the address (wherever it is referred) from all the address sets; otherwise, the system will cause a commit failure.

Address Books and Security Zones

A security zone is a logical group of interfaces with identical security requirements. You attach security zones to address books that contain entries for the addressable networks and end hosts (and, thus, users) belonging to the zone.

A zone can use two address books at a time—the global address book and the address book that the zone is attached to. When a security zone is not attached to any address book, it automatically uses the global address book. Thus, when a security zone is attached to an address book, the system looks up addresses from this attached address book; otherwise, the system looks up addresses from the default global address book. The global address book is available to all security zones by default; you do not need to attach zones to the global address book.

The following guidelines apply when attaching security zones to address books:

- Addresses attached to a security zone conform to the security requirements of the zone.
- The address book that you attach to a security zone must contain all IP addresses that are reachable within that zone.
- When you configure policies between two zones, you must define the addresses for each of the zone's address books.
- Addresses in a user-defined address book have a higher lookup priority than addresses in the global address book. Thus, for a security zone that is attached to a user-defined address book, the system searches the user-defined address book first; if no address is found, then it searches the global address book.

Address Books and Security Policies

Addresses and address sets are used when specifying the match criteria for a policy. Before you can configure policies to permit, deny, or tunnel traffic to and from individual hosts and subnets, you must make entries for them in address books. You can define different types of addresses, such as IPv4 addresses, IPv6 addresses, wildcard addresses, and DNS names, as match criteria for security policies.

Policies contain both source and destination addresses. You can refer to an address or address set in a policy by the name you give to it in the address book attached to the zone specified in the policy.

- When traffic is sent to a zone, the zone and address to which the traffic is sent are used as the destination zone and address-matching criteria in policies.
- When traffic is sent from a zone, the zone and address from which the traffic is sent are used as the source zone and address-matching criteria in policies.

Addresses Available for Security Policies

When configuring the source and destination addresses for a policy rule, you can type a question mark in the CLI to list all the available addresses that you can choose from.

You can use the same address name for different addresses that are in different address books. However, the CLI lists only one of these addresses—the address that has the highest lookup priority.

For example, suppose you configure addresses in two address books—**global** and **book1**. Then, display the addresses that you can configure as source or destination addresses in a policy (see Table 4 on page 50).

Table 4: Available Addresses Displayed in the CLI

Addresses Configured	Addresses Displayed in the CLI

[edit security address-book]
set global address a1 203.0.113.0/24;
set global address a2 198.51.100.0/24;
set global address a3 192.0.2.0/24;
set book1 address a1 203.113..128/25;
	`[edit security policies from-zone trust to-zone untrust]`
	`user@host#` **set policy p1 match set match source-address ?**
	
	`Possible completions:`
	`  [         Open a set of values`
	`  a1        The address in address book book1`
	`  a2        The address in address book global`
	`  a3        The address in address book global`
	`  any       Any IPv4 or IPv6 address`
	`  any-ipv4  Any IPv4 address`
	`  any-ipv6  Any IPv6 address`

The addresses displayed in this example illustrate:

- Addresses in a user-defined address book have a higher lookup priority than addresses in the global address book.

- Addresses in a global address book have a higher priority than the predefined addresses **any**, **any-ipv4**, and **any-ipv6**.
- When the same address name is configured for two or more different addresses, only the highest priority address, based on the address lookup, is available. In this example, the CLI displays address **a1** from **book1** (203.0.113.128/25) because that address has a higher lookup priority than the global address **a1** (203.0.113.0/24).

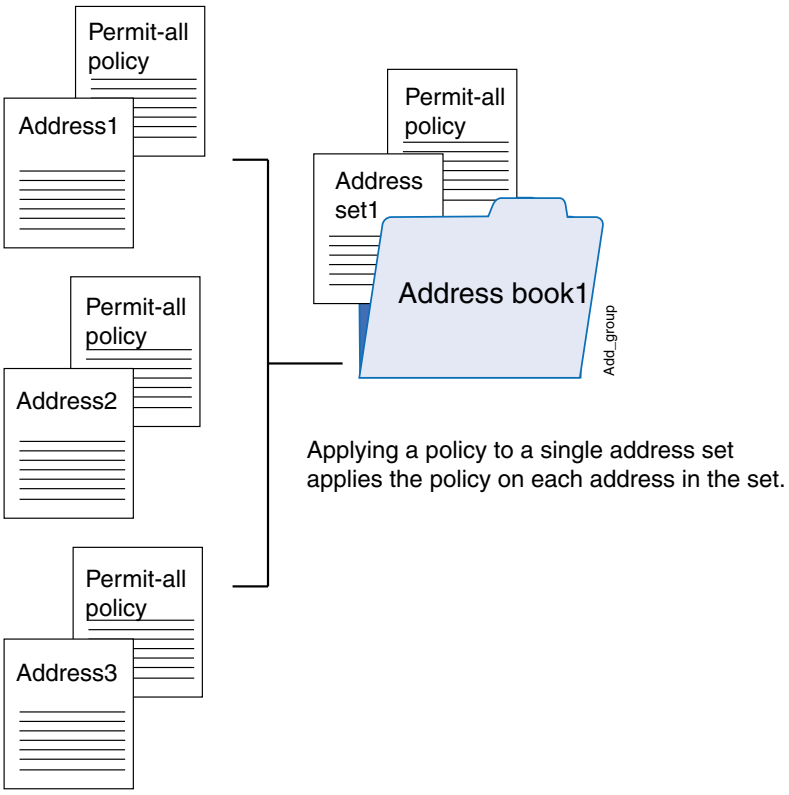
Applying Policies to Address Sets

When you specify an address set in policies, Junos OS applies the policies automatically to each address set member, so you do not have to create them one by one for each address. Also, if an address set is referenced in a policy, the address set cannot be removed without removing its reference in the policy. It can, however, be edited.

> **NOTE:** Consider that for each address set, the system creates individual rules for its members. It creates an internal rule for each member in the group as well as for each service configured for each user. If you configure address books without taking this into account, you can exceed the number of available policy resources, especially if both the source and destination addresses are address groups and the specified service is a service group.

Figure 2 on page 52 shows how policies are applied to address sets.

Figure 2: Applying Policies to Address Sets



Address Books and NAT

Once you define addresses in address books, you can specify them in the source, destination, or static NAT rules. It is simpler to specify meaningful address names instead of IP prefixes as source and destination addresses in the NAT rule configuration. For example, instead of specifying 10.208.16.0/22 as source address, you can specify an address called **local** that includes address 10.208.16.0/22.

You can also specify address sets in NAT rules, allowing you to add multiple addresses within an address set and therefore manage a small number of address sets, rather than manage a large number of individual address entries. When you specify an address set in a NAT rule, Junos OS applies the rule automatically to each address set member, so you do not have to specify each address one by one.

NOTE: The following address and address set types are not supported in NAT rules—wildcard addresses, DNS names, and a combination of IPv4 and IPv6 addresses.

When configuring address books with NAT, follow these guidelines:

- In a NAT rule, you can specify addresses from a global address book only. User-defined address books are not supported with NAT.

- You can configure an address set as a source address name in a source NAT rule. However, you cannot configure an address set as a destination address name in a destination NAT rule.

  The following sample NAT statements show the address and address set types that are supported with source and destination NAT rules:

  ```
  [edit security nat source rule-set src-nat rule src-rule1]
  set match source-address 2001:db8.1::/64
  set match source-address-name add1
  set match source-address-name add-set1
  set match destination-address 2001:db8::/64
  set match destination-address-name add2
  set match destination-address-name add-set2
  ```

  ```
  [edit security nat destination rule-set dst-nat rule dst-rule1]
  set match source-address 2001:db8::/64
  set match source-address-name add2
  set match source-address-name add-set2
  set match destination-address-name add1
  ```

- In a static NAT rule, you cannot configure an address set as a source or destination address name. The following sample NAT statements show the types of address that are supported with static NAT rules:

  ```
  [edit security nat static rule-set stat]
  set rule stat-rule1 match destination-address 203.0.113.0/24
  set rule stat-rule2 match destination-address-name add1
  ```

Example: Configuring Address Books and Address Sets

IN THIS SECTION

- Requirements | 54
- Overview | 54
- Configuration | 55
- Verification | 58

This example shows how to configure addresses and address sets in address books. It also shows how to attach address books to security zones.

Requirements

Before you begin:

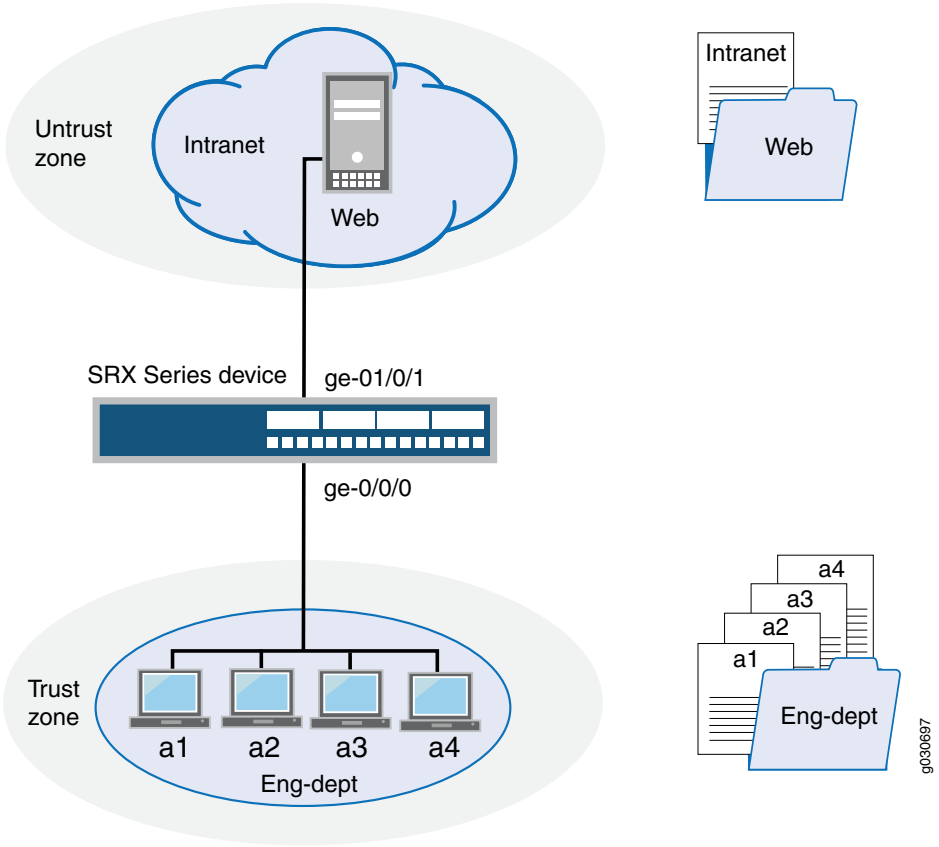
- Configure the Juniper Networks security devices for network communication.
- Configure network interfaces on server and member devices. See the *Interfaces User Guide for Security Devices*.
- Configure Domain Name System (DNS) services. For information about DNS, see *DNS Overview*.

Overview

In this example, you configure an address book with addresses and address sets (see Figure 3 on page 55) to simplify configuring your company's network. You create an address book called **Eng-dept** and add addresses of members from the Engineering department. You create another address book called **Web** and add a DNS name to it. Then you attach a security zone trust to the **Eng-dept** address book and security zone untrust to the **Web** address book. You also create address sets to group software and hardware addresses in the Engineering department. You plan to use these addresses as source address and destination addresses in your future policy configurations.

In addition, you add an address to the global address book, to be available to any security zone that has no address book attached to it.

Figure 3: Configuring Addresses and Address Sets



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 203.0.113.5
set interfaces ge-0/0/1 unit 0 family inet address 203.0.113.6
set security zones security-zone trust interfaces ge-0/0/0
set security zones security-zone untrust interfaces ge-0/0/1
set security address-book Eng-dept address a1 203.0.113.1
set security address-book Eng-dept address a2 203.0.113.2
set security address-book Eng-dept address a3 203.0.113.3
set security address-book Eng-dept address a4 203.0.113.4
set security address-book Eng-dept address-set sw-eng address a1
set security address-book Eng-dept address-set sw-eng address a2
set security address-book Eng-dept address-set hw-eng address a3
```

```
set security address-book Eng-dept address-set hw-eng address a4
set security address-book Eng-dept attach zone trust
set security address-book Web address Intranet dns-name www-int.device1.example.com
set security address-book Web attach zone untrust
set security address-book global address g1 198.51.100.2
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure addresses and address sets:

1. Configure Ethernet interfaces and assign IPv4 addresses to them.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 203.0.113.5
user@host# set interfaces ge-0/0/1 unit 0 family inet address 203.0.113.6
```

2. Create security zones and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/0
user@host# set security zones security-zone untrust interfaces ge-0/0/1
```

3. Create an address book and define addresses in it.

```
[edit security address-book Eng-dept ]
user@host# set address a1 203.0.113.1
user@host# set address a2 203.0.113.2
user@host# set address a3 203.0.113.3
user@host# set address a4 203.0.113.4
```

4. Create address sets.

```
[edit security address-book Eng-dept]
user@host# set address-set sw-eng address a1
user@host# set address-set sw-eng address a2
user@host# set address-set hw-eng address a3
user@host# set address-set hw-eng address a4
```

5. Attach the address book to a security zone.

```
[edit security address-book Eng-dept]
user@host# set attach zone trust
```

6. Create another address book and attach it to a security zone.

```
[edit security address-book Web ]
user@host# set address Intranet dns-name www-int.device1.example.com
user@host# set attach zone untrust
```

7. Define an address in the global address book.

```
[edit]
user@host# set security address-book global address g1 198.51.100.2
```

Results

From configuration mode, confirm your configuration by entering the **show security zones** and **show security address-book** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security zones
   security-zone trust {
      interfaces {
         ge-0/0/0.0;
      }
   }
   security-zone untrust {
      interfaces {
         ge-0/0/1.0;
      }
   }
[edit]
user@host# show security address-book
      Eng-dept {
         address a1 203.0.113.1/32;
         address a2 203.0.113.2/32;
         address a3 203.0.113.3/32;
         address a4 203.0.113.4/32;
         address-set sw-eng {
```

```
        address a1;
        address a2;
    }
    address-set hw-eng {
        address a3;
        address a4;
    }
    attach {
        zone trust;
    }
}
    Web {
        address Intranet {
            dns-name www-int.device1.example.com;
        }
        attach {
            zone untrust;
        }
    }
    global {
        address g1 198.51.100.2/32;
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Address Book Configuration | **58**
- Verifying Global Address Book Configuration | **59**

Confirm that the configuration is working properly.

Verifying Address Book Configuration

Purpose

Display information about configured address books and addresses.

Action

From configuration mode, enter the **show security address-book** command.

user@host# show security address-book

```
Eng-dept {
    address a1 203.0.113.1/32;
    address a2 203.0.113.2/32;
    address a3 203.0.113.3/32;
    address a4 203.0.113.4/32;
    address-set sw-eng {
        address a1;
        address a2;
    }
    address-set hw-eng {
        address a3;
        address a4;
    }
    attach {
        zone trust;
    }
}
Web {
    address Intranet {
        dns-name www-int.device1.example.com;
    }
    attach {
        zone untrust;
    }
}
global {
    address g1 198.51.100.2/32;
}
```

Verifying Global Address Book Configuration

Purpose

Display information about configured addresses in the global address book.

Action

From configuration mode, enter the **show security address-book global** command.

user@host# show security address-book global

```
address g1 198.51.100.2/32;
```

Excluding Addresses from Policies

Junos OS allows users to add any number of source and destination addresses to a policy. If you need to exclude certain addresses from a policy, you can configure them as negated addresses. When an address is configured as a negated address, it is excluded from a policy. You cannot, however, exclude the following IP addresses from a policy:

- Wildcard
- IPv6
- any
- any-ipv4
- any-ipv6
- 0.0.0.0

When a range of addresses or a single address is negated, it can be divided into multiple addresses. These negated addresses are shown as a prefix or a length that requires more memory for storage on a Packet Forwarding Engine.

Each platform has a limited number of policies with negated addresses. A policy can contain 10 source or destination addresses. The capacity of the policy depends on the maximum number of policies that the platform supports.

Before you configure a negated source address, destination address, or both, perform the following tasks:

1. Create a source, destination, or both address book.
2. Create address names and assign source and destination addresses to the address names.
3. Create address sets to group source, destination, or both address names.
4. Attach source and destination address books to security zones. For example, attach the source address book to the from-zone **trust** and the destination address book to the to-zone **untrust**.
5. Specify the match source, destination, or both address names.
6. Execute source-address-excluded, destination-address excluded, or both commands. A source, destination, or both addresses added in the source, destination, or both address books will be excluded from the policy.

> **NOTE:** The global address book does not need to be attached to any security zone.

Example: Excluding Addresses from Policies

IN THIS SECTION

- Requirements | **61**
- Overview | **62**
- Configuration | **62**
- Verification | **65**

This example shows how to configure negated source and destination addresses. It also shows how to configure address books and address sets.

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- A PC

- Junos OS Release 12.1X45-D10

Before you begin, configure address books and address sets. See "Example: Configuring Address Books and Address Sets" on page 53.

Overview

In this example, you create source and destination address books, SOUR-ADDR and DES-ADDR, and add source and destination addresses to it. You create source and destination address sets, as1 and as2, and group source and destination addresses to them. Then you attach source address book to the security zone trust and the destination address book to the security zone untrust.

You create security zones from-zone trust and to-zone untrust. You specify the policy name to p1 and then you set the name of the match source address to as1 and the match destination address to as2. You specify the commands **source -address-excluded** and **destination -address-excluded** to exclude source and destination addresses configured in the policy p1. Finally, you set the policy p1 to permit traffic from-zone trust to to-zone untrust.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security address-book SOU-ADDR address ad1 255.255.255.255/32
set security address-book SOU-ADDR address ad2 203.0.113.130/25
set security address-book SOU-ADDR address ad3 range-address 192.0.2.6 to 192.0.2.116
set security address-book SOU-ADDR address ad4 192.0.2.128/25
set security address-book SOU-ADDR address-set as1 address ad1
set security address-book SOU-ADDR address-set as1 address ad2
set security address-book SOU-ADDR address-set as1 address ad3
set security address-book SOU-ADDR address-set as1 address ad4
set security address-book SOU-ADDR attach zone trust
set security address-book DES-ADDR address ad8 198.51.100.1/24
set security address-book DES-ADDR address ad9 range-address 192.0.2.117 to 192.0.2.199
set security address-book DES-ADDR address ad10 198.51.100.0/24
set security address-book DES-ADDR address ad11 range-address 192.0.2.199 to 192.0.2.250
set security address-book DES-ADDR address-set as2 address ad8
set security address-book DES-ADDR address-set as2 address ad9
set security address-book DES-ADDR address-set as2 address ad10
set security address-book DES-ADDR address-set as2 address ad11
set security address-book DES-ADDR attach zone untrust
set security policies from-zone trust to-zone untrust policy p1 match source-address as1
```

```
set security policies from-zone trust to-zone untrust policy p1 match source-address-excluded
set security policies from-zone trust to-zone untrust policy p1 match destination-address as2
set security policies from-zone trust to-zone untrust policy p1 match destination-address-excluded
set security policies from-zone trust to-zone untrust policy p1 match application any
set security policies from-zone trust to-zone untrust policy p1 then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure negated addresses:

1. Create a source address book and address names. Add the source addresses to the address book.

```
[edit security address book ]
user@host#set SOU-ADDR address ad1 255.255.255.255/32
user@host#set SOU-ADDR address ad2 203.0.113.130/25
user@host#set SOU-ADDR ad3 range-address 192.0.2.6 to 192.0.2.116
user@host#set SOU-ADDR address ad4 192.0.2.128/25
```

2. Create an address set to group source address names.

```
[edit security address book ]
user@host# set SOU-ADDR address-set as1 address ad1
user@host# set SOU-ADDR address-set as1 address ad2
user@host# set SOU-ADDR address-set as1 address ad3
user@host# set SOU-ADDR address-set as1 address ad4
```

3. Attach the source address book to the security from zone.

```
[edit security address book ]
user@host# set SOU-ADDR attach zone trust
```

4. Create a destination address book and address names. Add the destination addresses to the address book.

```
[edit security address book ]
user@host#set DES-ADDR address ad8 198.51.100.1/24
user@host#set DES-ADDR address ad9 range-address 192.0.2.117 to 192.0.2.199
user@host#set DES-ADDR address ad10 198.51.100.0/24
```

```
user@host#set DES-ADDR address ad11 range-address 192.0.2.199 to 192.0.2.250
```

5. Create another address set to group destination address names.

```
[edit security address book ]
user@host# set DES-ADDR address-set as1 address ad8
user@host# set DES-ADDR address-set as1 address ad9
user@host# set DES-ADDR address-set as1 address ad10
user@host# set DES-ADDR address-set as1 address ad11
```

6. Attach the destination address book to the security to zone.

```
[edit security address book ]
user@host# set DES-ADDR attach zone untrust
```

7. Specify the policy name and source address.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match source-address as1
```

8. Exclude source addresses from the policy.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match source-address-excluded
```

9. Specify the destination address.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match destination-address as2
```

10. Exclude destination addresses from the policy.

```
[edit security policies]
user@host#  set from-zone trust to-zone untrust policy p1 match destination-address-excluded
```

11. Configure the security policy application.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match application any
```

12. Permit the traffic from-zone trust to to-zone untrust.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
   from-zone trust to-zone untrust {
      policy p1 {
         match {
            source-address as1;
            destination-address as2;
            source-address-excluded;
            destination-address-excluded;
            application any;
         }
         then {
            permit;
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying the Policy Configuration | 66
- Verifying the Policy Configuration Detail | 66

Confirm that the configuration is working properly.

Verifying the Policy Configuration

Purpose

Verify that the policy configuration is correct.

Action

From operational mode, enter the **show security policies policy-name p1** command.

```
user@host>show security policies policy-name p1
```

```
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit
```

This output summarizes the policy configuration.

Verifying the Policy Configuration Detail

Purpose

Verify that the policy and the negated source and destination address configurations are correct.

Action

From operational mode, enter the **show security policies policy-name p1 detail** command.

```
user@host>show security policies policy-name p1 detail
```

```
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
    ad1(SOU-ADDR): 255.255.255.255/32
    ad2(SOU-ADDR): 203.0.113.130/25
    ad3(SOU-ADDR): 192.0.2.6 ~ 192.0.2.116
    ad4(SOU-ADDR): 192.0.2.128/25
    Destination addresses(excluded):
    ad8(DES-ADDR): 198.51.100.1/24
```

```
  ad9(DES-ADDR): 192.0.2.117 ~ 192.0.2.199
  ad10(DES-ADDR): 198.51.100.0/24
  ad11(DES-ADDR): 192.0.2.199 to 192.0.2.250
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
```

This output summarizes the policy configuration and shows the names of negated source and destination addresses excluded from the policy.

SEE ALSO

Predefined Policy Applications | 75

Custom Policy Applications | 96

4

CHAPTER

Security Policy Applications and Application Sets

Security Policy Applications and Application Sets | 69

Predefined Policy Applications | 75

Custom Policy Applications | 96

Security Policy Applications and Application Sets

IN THIS SECTION

- Security Policy Applications Overview | 69
- Security Policy Application Sets Overview | 70
- Example: Configuring Security Policy Applications and Application Sets | 71
- Understanding Policy Application Timeout Configuration and Lookup | 72
- Understanding Policy Application Timeouts Contingencies | 73
- Example: Setting a Policy Application Timeout | 74

Policy applications are types of traffic for which protocol standards exist. The policy application set is a group of policy applications. Junos OS simplifies the process by allowing you to manage a small number of policy application sets, rather than a large number of individual policy application entries. The policy application or policy application set is referred to by security policies as match criteria for packets initiating sessions.

The policy application or application set is referred to by security policies as match criteria for packets initiating sessions. Junos OS allows you to configure policy applications and application sets. You can create an application set that contains all the approved applications.

Security Policy Applications Overview

Applications are types of traffic for which protocol standards exist. Each application has a transport protocol and destination port number(s) associated with it, such as TCP/port 21 for FTP and TCP/port 23 for Telnet. When you create a policy, you must specify an application for it.

You can select one of the predefined applications from the application book, or a custom application or application set that you created. You can see which application you can use in a policy by using the **show applications** CLI command.

NOTE: Each predefined application has a source port range of **1–65535**, which includes the entire set of valid port numbers. This prevents potential attackers from gaining access by using a source port outside of the range. If you need to use a different source port range for any predefined application, create a custom application. For information, see "Understanding Custom Policy Applications" on page 96.

SEE ALSO

Understanding Security Policy Elements | **105**

Security Policy Application Sets Overview

When you create a policy, you must specify an application, or service, for it to indicate that the policy applies to traffic of that type. Sometimes the same applications or a subset of them can be present in multiple policies, making it difficult to manage. Junos OS allows you to create groups of applications called application sets. Application sets simplify the process by allowing you to manage a small number of application sets, rather than a large number of individual application entries.

The application (or application set) is referred to by security policies as match criteria for packets initiating sessions. If the packet matches the application type specified by the policy and all other criteria match, then the policy action is applied to the packet.

You can specify the name of an application set in a policy. In this case, if all of the other criteria match, any one of the applications in the application set serves as valid matching criteria; **any** is the default application name that indicates all possible applications.

Applications are created in the **.../applications/application/*application-name*** directory. You do not need to configure an application for any of the services that are predefined by the system.

In addition to predefined services, you can configure a custom service. After you create a custom service, you can refer to it in a policy.

Example: Configuring Security Policy Applications and Application Sets

IN THIS SECTION

- Requirements | 71
- Overview | 71
- Configuration | 71
- Verification | 72

This example shows how to configure applications and application sets.

Requirements

Before you begin, configure the required applications. See "Security Policy Application Sets Overview" on page 70.

Overview

Rather than creating or adding multiple individual application names to a policy, you can create an application set and refer to the name of the set in a policy. For example, for a group of employees, you can create an application set that contains all the approved applications.

In this example, you create an application set that are used to log in to the servers in the ABC (intranet) zone, to access the database, and to transfer files.

- Define the applications in the configured application set.
- Managers in zone A and managers in zone B use these services. Therefore, give the application set a generic name, such as MgrAppSet.
- Create an application set for the applications that are used for e-mail and Web-based applications that are delivered by the two servers in the external zone.

Configuration

Step-by-Step Procedure

To configure an application and application set:

1. Create an application set for managers.

```
[edit applications]
user@host# set application-set MgrAppSet application junos-ssh
user@host# set application-set MgrAppSet application junos-telnet
```

2. Create another application set for e-mail and Web-based applications.

```
[edit applications]
user@host# set application-set WebMailApps application junos-smtp
user@host# set application-set WebMailApps application junos-pop3
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show applications** command in configuration mode.

Understanding Policy Application Timeout Configuration and Lookup

The application timeout value you set for an application determines the session timeout. You can set the timeout threshold for a predefined or custom application; you can use the application default timeout, specify a custom timeout, or use no timeout at all.

Application timeout values are stored in the root TCP and UDP port-based timeout table and in the protocol-based default timeout table. When you set an application timeout value, Junos OS updates these tables with the new value. There are also default timeout values in the applications entry database, which are taken from predefined applications. You can set a timeout, but you cannot alter a default value.

Each custom application can be configured with its own custom application timeout. If multiple custom applications are configured with custom timeouts, then each application will have its own custom application timeout.

If the application that is matched for the traffic has a timeout value, that timeout value is used. Otherwise, the lookup proceeds in the following order until an application timeout value is found:

1. The root TCP and UDP port-based timeout table is searched for a timeout value.

2. The protocol-based default timeout table is searched for a timeout value. See Table 5 on page 73.

Table 5: Protocol-Based Default Timeout

Protocol	Default Timeout (seconds)
TCP	1800
UDP	60
ICMP	60
OSPF	60
Other	1800

Understanding Policy Application Timeouts Contingencies

When setting timeouts, be aware of the following contingencies:

- If an application contains several application rule entries, all rule entries share the same timeout. You need to define the application timeout only once. For example, if you create an application with two rules, the following commands will set the timeout to **20** seconds for both rules:

```
user@host# set applications application test protocol tcp destination-port 1035-1035
inactivity-timeout 20
user@host# set applications application test term test protocol udp
user@host# set applications application test term test source-port 1-65535
user@host# set applications application test term test destination-port 1111-1111
```

- If multiple custom applications are configured with custom timeouts, then each application will have its own custom application timeout. For example:

```
user@host# set applications application ftp-1 protocol tcp source-port 0-65535 destination-port
2121-2121 inactivity-timeout 10
user@host# set applications application telnet-1 protocol tcp source-port 0-65535 destination-port
2300-2348 inactivity-timeout 20
```

With this configuration, Junos OS applies a 10-second timeout for destination port **2121** and a 20-second timeout for destination port **2300** in an application group.

Example: Setting a Policy Application Timeout

IN THIS SECTION

- Requirements | 74
- Overview | 74
- Configuration | 74
- Verification | 75

This example shows how to set a policy application timeout value.

Requirements

Before you begin, understand policy application timeouts. See "Understanding Policy Application Timeout Configuration and Lookup" on page 72.

Overview

Application timeout values are stored in the application entry database and in the corresponding vsys TCP and UDP port-based timeout tables. In this example, you set the device for a policy application timeout to 75 minutes for the FTP predefined application.

When you set an application timeout value, Junos OS updates these tables with the new value.

Configuration

Step-by-Step Procedure

To set a policy application timeout:

1. Set the inactivity timeout value.

```
[edit applications application ftp]
user@host# set inactivity-timeout 75
```

2. Commit the configuration if you are done configuring the device.

```
[edit]
```

```
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show applications** command.

RELATED DOCUMENTATION

- Custom Policy Applications | **96**

Predefined Policy Applications

IN THIS SECTION

- Understanding Internet-Related Predefined Policy Applications | **76**
- Understanding Microsoft Predefined Policy Applications | **78**
- Understanding Dynamic Routing Protocols Predefined Policy Applications | **79**
- Understanding Streaming Video Predefined Policy Applications | **79**
- Understanding Sun RPC Predefined Policy Applications | **80**
- Understanding Security and Tunnel Predefined Policy Applications | **81**
- Understanding IP-Related Predefined Policy Applications | **82**
- Understanding Instant Messaging Predefined Policy Applications | **82**
- Understanding Management Predefined Policy Applications | **83**
- Understanding Mail Predefined Policy Applications | **85**
- Understanding UNIX Predefined Policy Applications | **85**
- Understanding Miscellaneous Predefined Policy Applications | **86**
- Understanding ICMP Predefined Policy Applications | **87**
- Example: Defining a Custom ICMP Application | **93**

Predefined policy allows you to choose the applications to permit or deny. You can specify the predefined applications for the policy, depending on your network requirements.

Understanding Internet-Related Predefined Policy Applications

When you create a policy, you can specify predefined Internet-related applications for the policy.

Table 6 on page 76 lists Internet-related predefined applications. Depending on your network requirements, you can choose to permit or deny any or all of these applications. Each entry lists the application name, default receiving port, and application description.

Table 6: Predefined Applications

Application Name	Port(s)	Application Description
AOL	5190-5193	America Online Internet service provider (ISP) provides Internet, chat, and instant messaging applications.
DHCP relay	67 (default)	Dynamic Host Configuration Protocol.
DHCP	68 client 67 server	Dynamic Host Configuration Protocol allocates network addresses and delivers configuration parameters from server to hosts.
DNS	53	Domain Name System translates domain names into IP addresses.
FTP	20 data 21 control	File Transfer Protocol (FTP) allows the sending and receiving of files between machines. You can choose to deny or permit ANY or to selectively permit or deny. We recommend denying FTP applications from untrusted sources (Internet).
Gopher	70	Gopher organizes and displays Internet servers' contents as a hierarchically structured list of files. We recommend denying Gopher access to avoid exposing your network structure.
HTTP	80	HyperText Transfer Protocol is the underlying protocol used by the World Wide Web (WWW). Denying HTTP application disables your users from viewing the Internet. Permitting HTTP application allows your trusted hosts to view the Internet.
HTTP-EXT	—	Hypertext Transfer Protocol with extended nonstandard ports

Table 6: Predefined Applications *(continued)*

Application Name	Port(s)	Application Description
HTTPS	443	Hypertext Transfer Protocol with Secure Sockets Layer (SSL) is a protocol for transmitting private documents through the Internet. Denying HTTPS disables your users from shopping on the Internet and from accessing certain online resources that require secure password exchange. Permitting HTTPS allows your trusted hosts to participate in password exchange, shop online, and visit various protected online resources that require user login.
Internet Locator Service	—	Internet Locator Service includes LDAP, User Locator Service, and LDAP over TSL/SSL.
IRC	6665-6669	Internet Relay Chat (IRC) allows people connected to the Internet to join live discussions.
LDAP	389	Lightweight Directory Access Protocol is a set of protocols used to access information directories.
PC-Anywhere	—	PC-Anywhere is a remote control and file transfer software.
TFTP	69	Trivial File transfer Protocol (TFTP) is a protocol for simple file transfer.
WAIS	—	Wide Area Information Server is a program that finds documents on the Internet.

NOTE: Starting in Junos OS Release Junos OS Release 18.4R1, encrypted applications such as HTTP, SMTP, IMAP and POP3 over SSL are identified as junos:HTTPS, junos:SMTPS, junos:IMAPS, and junos:POP3S in Junos OS predefined applications and application sets. For example: If you configure a security policy to allow or deny HTTPS traffic, you must specify application matching criteria as junos:HTTPS. In previous Junos OS Releases, both HTTP and encrypted HTTP (HTTPS) applications can be configured using a same application matching criteria as junos:HTTP.

Understanding Microsoft Predefined Policy Applications

When you create a policy, you can specify predefined Microsoft applications for the policy.

Table 7 on page 78 lists predefined Microsoft applications, parameters associated with each application, and a brief description of each application. Parameters include universal unique identifiers (UUIDs) and TCP/UDP source and destination ports. A UUID is a 128-bit unique number generated from a hardware address, a timestamp, and seed values.

Table 7: Predefined Microsoft Applications

Application	Parameter/UUID	Description
Junos MS-RPC-EPM	135 e1af8308-5d1f-11c9-91a4-08002b14a0fa	Microsoft remote procedure call (RPC) Endpoint Mapper (EPM) Protocol.
Junos MS-RPC	—	Any Microsoft remote procedure call (RPC) applications.
Junos MS-RPC-MSEXCHANGE	3 members	Microsoft Exchange application group includes: • Junos-MS-RPC-MSEXCHANGE-DATABASE • Junos-MS-RPC-MSEXCHANGE-DIRECTORY • Junos-MS-RPC-MSEXCHANGE-INFO-STORE
Junos-MS-RPC-MSEXCHANGE-DATABASE	1a190310-bb9c-11cd-90f8-00aa00466520	Microsoft Exchange Database application.
Junos-MS-RPC-MSEXCHANGE-DIRECTORY	f5cc5a18-4264-101a-8c59-08002b2f8426 f5cc5a7c-4264-101a-8c59-08002b2f8426 f5cc59b4-4264-101a-8c59-08002b2f8426	Microsoft Exchange Directory application.
Junos-MS-RPC-MSEXCHANGE-INFO-STORE	0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde 1453c42c-0fa6-11d2-a910-00c04f990f3b 10f24e8e-0fa6-11d2-a910-00c04f990f3b 1544f5e0-613c-11d1-93df-00c04fd7bd09	Microsoft Exchange Information Store application.
Junos-MS-RPC-TCP	—	Microsoft Transmission Control Protocol (TCP) application.

Table 7: Predefined Microsoft Applications *(continued)*

Application	Parameter/UUID	Description
Junos-MS-RPC-UDP	—	Microsoft User Datagram Protocol (UDP) application.
Junos-MS-SQL	—	Microsoft Structured Query Language (SQL).
Junos-MSN	—	Microsoft Network Messenger application.

Understanding Dynamic Routing Protocols Predefined Policy Applications

When you create a policy, you can specify predefined dynamic routing protocol applications for the policy.

Depending on your network requirements, you can choose to permit or deny messages generated from these dynamic routing protocols and packets of these dynamic routing protocols. Table 8 on page 79 lists each supported dynamic routing protocol by name, port, and description.

Table 8: Dynamic Routing Protocols

Dynamic Routing Protocol	Port	Description
RIP	520	RIP is a common distance-vector routing protocol.
OSPF	89	OSPF is a common link-state routing protocol.
BGP	179	BGP is an exterior/interdomain routing protocol.

Understanding Streaming Video Predefined Policy Applications

When you create a policy, you can specify predefined streaming video applications for the policy.

Table 9 on page 80 lists each supported streaming video application by name and includes the default port and description. Depending on your network requirements, you can choose to permit or deny any or all of these applications.

Table 9: Supported Streaming Video Applications

Application	Port	Description
H.323	TCP source 1-65535; TCP destination 1720, 1503, 389, 522, 1731 UDP source 1-65535; UDP source 1719	H.323 is a standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conference data is transmitted across networks.
NetMeeting	TCP source 1-65535; TCP destination 1720, 1503, 389, 522 UDP source 1719	Microsoft NetMeeting uses TCP to provide teleconferencing (video and audio) applications over the Internet.
Real media	TCP source 1-65535; TCP destination 7070	Real Media is streaming video and audio technology.
RTSP	554	Real-Time Streaming Protocol (RTSP) is for streaming media applications
SIP	5056	Session Initiation Protocol (SIP) is an Application-Layer control protocol for creating, modifying, and terminating sessions.
VDO Live	TCP source 1-65535; TCP destination 7000-7010	VDOLive is a scalable, video streaming technology.

Understanding Sun RPC Predefined Policy Applications

When you create a policy, you can specify predefined Sun RPC applications for the policy.

Table 10 on page 80 lists each Sun remote procedure call Application Layer Gateway (RPC ALG) application name, parameters, and full name.

Table 10: RPC ALG Applications

Application	Program Numbers	Full Name
SUN-RPC-PORTMAPPER	111100000	Sun RPC Portmapper protocol
SUN-RPC-ANY	ANY	Any Sun RPC applications
SUN-RPC-PROGRAM-MOUNTD	100005	Sun RPC Mount Daemon

Table 10: RPC ALG Applications *(continued)*

Application	Program Numbers	Full Name
SUN-RPC-PROGRAM-NFS	100003 100227	Sun RPC Network File System
SUN-RPC-PROGRAM-NLOCKMGR	100021	Sun RPC Network Lock Manager
SUN-RPC-PROGRAM-RQUOTAD	100011	Sun RPC Remote Quota Daemon
SUN-RPC-PROGRAM-RSTATD	100001	Sun RPC Remote Status Daemon
SUN-RPC-PROGRAM-RUSERD	100002	Sun RPC Remote User Daemon
SUN-RPC-PROGRAM-SADMIND	100232	Sun RPC System Administration Daemon
SUN-RPC-PROGRAM-SPRAYD	100012	Sun RPC Spray Daemon
SUN-RPC-PROGRAM-STATUS	100024	Sun RPC Status
SUN-RPC-PROGRAM-WALLD	100008	Sun RPC Wall Daemon
SUN-RPC-PROGRAM-YPBIND	100007	SUN RPC Yellow Page Bind application

Understanding Security and Tunnel Predefined Policy Applications

When you create a policy, you can specify predefined security and tunnel applications for the policy.

Table 11 on page 81 lists each supported application and gives the default port(s) and a description of each entry.

Table 11: Supported Applications

Application	Port	Description
IKE	UDP source 1-65535; UDP destination 500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite. Internet Key protocol (IKE) is a protocol to obtain authenticated keying material for use with ISAKMP.

Table 11: Supported Applications *(continued)*

Application	Port	Description
IKE-NAT	4500	IKE-Network Address Translation (NAT) performs Layer 3 NAT for S2C IKE traffic.
L2TP	1701	L2TP combines PPTP with Layer 2 Forwarding (L2F) for remote access.
PPTP	1723	Point-to-Point Tunneling Protocol allows corporations to extend their own private network through private *tunnels* over the public Internet.

Understanding IP-Related Predefined Policy Applications

When you create a policy, you can specify predefined IP-related applications for the policy.

Table 12 on page 82 lists the predefined IP-related applications. Each entry includes the default port and a description of the application.

TCP-ANY means any application that is using TCP, so there is no default port for it. The same is true for UDP-ANY.

Table 12: Predefined IP-Related Applications

Application	Port	Description
Any	—	Any application
TCP-ANY	0-65,535	Any protocol using the TCP
UDP-ANY	0-65,535	Any protocol using the UDP

Understanding Instant Messaging Predefined Policy Applications

When you create a policy, you can specify predefined instant messaging applications for the policy.

Table 13 on page 83 lists predefined Internet-messaging applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 13: Predefined Internet-Messaging Applications

Application	Port	Description
Gnutella	6346 (default)	Gnutella is a public domain file sharing protocol that operates over a distributed network. You can assign any port, but the default is 6346.
MSN	1863	Microsoft Network Messenger is a utility that allows you to send instant messages and talk online.
NNTP	119	Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages.
SMB	445	Server Message Block (SMB) over IP is a protocol that allows you to read and write files to a server on a network.
YMSG	5010	Yahoo! Messenger is a utility that allows you to check when others are online, send instant messages, and talk online.

Understanding Management Predefined Policy Applications

When you create a policy, you can specify predefined management applications for the policy.

Table 14 on page 83 lists the predefined management applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 14: Predefined Management Applications

Application	Port	Description
NBNAME	137	NetBIOS Name application displays all NetBIOS name packets sent on UDP port 137.
NDBDS	138	NetBIOS Datagram application, published by IBM, provides connectionless (datagram) applications to PCs connected with a broadcast medium to locate resources, initiate sessions, and terminate sessions. It is unreliable and the packets are not sequenced.
NFS	—	Network File System uses UDP to allow network users to access shared files stored on computers of different types. SUN RPC is a building block of NFS.

Table 14: Predefined Management Applications *(continued)*

Application	Port	Description
NS Global	—	NS-Global is the central management protocol for Juniper Networks Firewall/VPN devices.
NS Global PRO	—	NS Global-PRO is the scalable monitoring system for the Juniper Networks Firewall/VPN device family.
NSM	—	Network and Security Manager
NTP	123	Network Time Protocol provides a way for computers to synchronize to a time reference.
RLOGIN	513	RLOGIN starts a terminal session on a remote host.
RSH	514	RSH executes a shell command on a remote host.
SNMP	161	Simple Network Management Protocol is a set of protocols for managing complex networks.
SQL*Net V1	66	SQL*Net Version 1 is a database language that allows for the creation, access, modification, and protection of data.
SQL*Net V2	66	SQL*Net Version 2 is a database language that allows for the creation, access, modification, and protection of data.
MSSQL	1433 (default instance)	Microsoft SQL is a proprietary database server tool that allows for the creation, access, modification, and protection of data.
SSH	22	SSH is a program to log in to another computer over a network through strong authentication and secure communications on an unsecure channel.
SYSLOG	514	Syslog is a UNIX program that sends messages to the system logger.
Talk	517-518	Talk is a visual communication program that copies lines from your terminal to that of another user.
Telnet	23	Telnet is a UNIX program that provides a standard method of interfacing terminal devices and terminal-oriented processes to each other.

Table 14: Predefined Management Applications *(continued)*

Application	Port	Description
WinFrame	—	WinFrame is a technology that allows users on non-Windows machines to run Windows applications.
X-Windows	—	X-Windows is the windowing and graphics system that Motif and OpenLook are based on.

Understanding Mail Predefined Policy Applications

When you create a policy, you can specify predefined mail applications for the policy.

Table 15 on page 85 lists the predefined mail applications. Each includes the name of the application, the default or assigned port number, and a description of the application.

Table 15: Predefined Mail Applications

Application	Port	Description
IMAP	143	Internet Message Access Protocol is used for retrieving messages.
Mail (SMTP)	25	Simple Mail Transfer Protocol is used to send messages between servers.
POP3	110	Post Office Protocol is used for retrieving e-mail.

Understanding UNIX Predefined Policy Applications

When you create a policy, you can specify predefined UNIX applications for the policy.

Table 16 on page 85 lists the predefined UNIX applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 16: Predefined UNIX Applications

Application	Port	Description
FINGER	79	Finger is a UNIX program that provides information about the users.

Table 16: Predefined UNIX Applications *(continued)*

Application	Port	Description
UUCP	117	UNIX-to-UNIX Copy Protocol (UUCP) is a UNIX utility that enables file transfers between two computers over a direct serial or modem connection.

Understanding Miscellaneous Predefined Policy Applications

When you create a policy, you can specify miscellaneous predefined applications for the policy.

Table 17 on page 86 lists predefined miscellaneous applications. Each entry includes the application name, default or assigned port, and a description of the application.

Table 17: Predefined Miscellaneous Applications

Application	Port	Description
CHARGEN	19	Character Generator Protocol is a UDP- or TCP-based debugging and measurement tool.
DISCARD	9	Discard protocol is an Application Layer protocol that describes a process for discarding TCP or UDP data sent to port 9.
IDENT	113	Identification protocol is a TCP/IP Application Layer protocol used for TCP client authentication.
LPR	515 listen; 721-731 source range (inclusive)	Line Printer Daemon protocol is a TCP-based protocol used for printing applications.
RADIUS	1812	Remote Authentication Dial-In User Service application is a server program used for authentication and accounting purposes.
RADIUS Accounting	1813	A RADIUS Accounting server receives statistical data about users logging in to or out of a LAN.
SQLMON	1434 (SQL Monitor Port)	SQL monitor (Microsoft)

Table 17: Predefined Miscellaneous Applications *(continued)*

Application	Port	Description
VNC	5800	Virtual Network Computing facilitates viewing and interacting with another computer or mobile Juniper Networks device connected to the Internet.
WHOIS	43	Network Directory Application Protocol is a way to look up domain names.
SCCP	2000	Cisco Station Call Control Protocol (SCCP) uses the signaling connection control port to provide high availability and flow control.

Understanding ICMP Predefined Policy Applications

When you create a policy, you can specify the ICMP predefined application for the policy.

Internet Control Message Protocol (ICMP) is a part of IP and provides a way to query a network (ICMP query messages) and to receive feedback from the network for error patterns (ICMP error messages). ICMP does not, however, guarantee error message delivery or report all lost datagrams; and it is not a reliable protocol. ICMP codes and type codes describe ICMP query messages and ICMP error messages.

You can choose to permit or deny any or specific types of ICMP messages to improve network security. Some types of ICMP messages can be exploited to gain information about your network that might compromise security. For example, ICMP, TCP, or UDP packets can be constructed to return ICMP error messages that contain information about a network, such as its topology, and access list filtering characteristics. Table 18 on page 87 lists ICMP message names, the corresponding code, type, and description.

Table 18: ICMP Messages

ICMP Message Name	Type	Code	Description
ICMP-ANY	all	all	ICMP-ANY affects any protocol using ICMP. Denying ICMP-ANY impairs any attempt to ping or monitor a network using ICMP. Permitting ICMP-ANY allows all ICMP messages.

Table 18: ICMP Messages *(continued)*

ICMP Message Name	Type	Code	Description
ICMP-ADDRESS-MASK • Request • Reply	17 18	0 0	ICMP address mask query is used for systems that need the local subnet mask from a bootstrap server. Denying ICMP address mask request messages can adversely affect diskless systems. Permitting ICMP address mask request messages might allow others to fingerprint the operating system of a host in your network.
ICMP-DEST-UNREACH	3	0	ICMP destination unreachable error message indicates that the destination host is configured to reject the packets. Codes 0, 1, 4, or 5 can be from a gateway. Codes 2 or 3 can be from a host (RFC 792). Denying ICMP destination unreachable error messages can remove the assumption that a host is up and running behind an SRX Series device. Permitting ICMP destination unreachable error messages can allow some assumptions, such as security filtering, to be made about the network.
ICMP Fragment Needed	3	4	ICMP fragmentation error message indicates that fragmentation is needed but the don't fragment flag is set. We recommend denying these messages from the Internet to an internal network.

Table 18: ICMP Messages *(continued)*

ICMP Message Name	Type	Code	Description
ICMP FragmentReassembly	11	1	ICMP fragment reassembly time exceeded error indicates that a host reassembling a fragmented message ran out of time and dropped the packet. This message is sometimes sent. We recommend denying these messages from the Internet (external) to the trusted (internal) network.
ICMP-HOST-UNREACH	3	1	ICMP host unreachable error messages indicate that routing table entries do not list or list as infinity a particular host. Sometimes this error is sent by gateways that cannot fragment when a packet requiring fragmentation is received. We recommend denying these messages from the Internet to a trusted network. Permitting these messages allows others to be able to determine your internal hosts IP addresses by a process of elimination or make assumptions about gateways and fragmentation.
ICMP-INFO • Request • Reply	15 16	0 0	ICMP-INFO query messages allow diskless host systems to query the network and self-configure. Denying ICMP address mask request messages can adversely affect diskless systems. Permitting ICMP address mask request messages might allow others to broadcast information queries to a network segment to determine computer type.

Table 18: ICMP Messages *(continued)*

ICMP Message Name	Type	Code	Description
ICMP-PARAMETER-PROBLEM	12	0	ICMP parameter problem error messages notify you when incorrect header parameters are present and have caused a packet to be discarded We recommend denying these messages from the Internet to a trusted network. Permitting ICMP parameter problem error messages allows others to make assumptions about your network.
ICMP-PORT-UNREACH	3	3	ICMP port unreachable error messages indicate that gateways processing datagrams requesting certain ports are unavailable or unsupported in the network. We recommend denying these messages from the Internet to a trusted network. Permitting ICMP port unreachable error messages can allow others to determine which ports you use for certain protocols.
ICMP-PROTOCOL-UNREACH	3	2	ICMP protocol unreachable error messages indicate that gateways processing datagrams requesting certain protocols are unavailable or unsupported in the network. We recommend denying these messages from the Internet to a trusted network. Permitting ICMP protocol unreachable error messages can allow others to determine what protocols your network is running.
ICMP-REDIRECT	5	0	ICMP redirect network error messages are sent by an SRX Series device. We recommend denying these messages from the Internet to a trusted network.

Table 18: ICMP Messages *(continued)*

ICMP Message Name	Type	Code	Description
ICMP-REDIRECT-HOST	5	1	ICMP redirect messages indicate datagrams destined for the specified host to be sent along another path.
ICMP-REDIRECT-TOS-HOST	5	3	ICMP redirect type of service (TOS) and host error is a type of message.
ICMP-REDIRECT-TOS-NET	5	2	ICMP redirect TOS and network error is a type of message.
ICMP-SOURCE-QUENCH	4	0	ICMP source quench error message indicates that a device does not have the buffer space available to accept, queue, and send the packets on to the next hop. Denying these messages will not help or impair internal network performance. Permitting these messages can allow others to know that a device is congested, making it a viable attack target.
ICMP-SOURCE-ROUTE-FAIL	3	5	ICMP source route failed error message We recommend denying these messages from the Internet (external).
ICMP-TIME-EXCEEDED	11	0	ICMP time-to-live (TTL) exceeded error message indicates that a packet's TTL setting reached zero before the packet reached its destination. This ensures that older packets are discarded before resent ones are processed. We recommend denying these messages from a trusted network out to the Internet.
ICMP-TIMESTAMP • Request • Reply	13 14	0 0	ICMP-TIMESTAMP query messages provide the mechanism to synchronize time and coordinate time distribution in a large, diverse network.

Table 18: ICMP Messages *(continued)*

ICMP Message Name	Type	Code	Description
Ping (ICMP ECHO)	8	0	Ping is a utility to determine whether a specific host is accessible by its IP address. Denying ping functionality removes your ability to check to see if a host is active. Permitting ping can allow others to execute a denial-of-service (DoS) or Smurf attack.
ICMP-ECHO-FRAGMENT-ASSEMBLY-EXPIRE	11	1	ICMP fragment echo reassembly time expired error message indicates that the reassembly time was exceeded. We recommend denying these messages.
Traceroute • Forward • Discard	30 30	0 1	Traceroute is a utility to indicate the path to access a specific host. We recommend denying this utility from the Internet (external) to your trusted network (internal).

Default Behavior of ICMP Unreachable Errors

For different levels of security, the default behavior for ICMP unreachable errors is handled as follows:

- Sessions are closed for ICMP type-3, code-0, code-1, code-2, and code-3 messages only when the following conditions are met:
  - The ICMP unreachable message is received in the server–to-client direction.
  - No normal packet is received in the server-to-client direction.

  Otherwise, sessions do not close.
- Sessions do not close for ICMP type-3, code-4 messages.

Example: Defining a Custom ICMP Application

IN THIS SECTION

- Requirements | 94
- Overview | 94
- Configuration | 95
- Verification | 95

This example shows how to define a custom ICMP application.

Requirements

Before you begin:

- Understand custom policy application. See "Understanding Custom Policy Applications" on page 96.
- Understand the ICMP predefined policy application. See "Understanding ICMP Predefined Policy Applications" on page 87.

Overview

Junos OS supports ICMP—as well as several ICMP messages—as predefined or custom applications. When configuring a custom ICMP application, you define a type and code.

- There are different message types within ICMP. For example:
  - type 0 = Echo Request message
  - type 3 = Destination Unreachable message
- An ICMP message type can also have a message code. The code provides more specific information about the message, as shown in Table 19 on page 94.

Table 19: Message Descriptions

Message Type	Message Code
5 = Redirect	0 = Redirect datagram for the network (or subnet)
	1 = Redirect datagram for the host
	2 = Redirect datagram for the type of application and network
	3 = Redirect datagram for the type of application and host
11 = Time Exceeded Codes	0 = Time to live exceeded in transit
	1 = Fragment reassembly time exceeded

Junos OS supports any type or code within the range of **0** through **55** .

In this example, you define a custom application named host-unreachable using ICMP as the transport protocol. The type is 3 (for destination unreachable) and the code is 1 (for host unreachable). You set the timeout value at 4 minutes.

NOTE: For more information about ICMP types and codes, refer to RFC 792, *Internet Control Message Protocol*.

Configuration

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To define a custom ICMP application:

1. Set the application type and code.

```
[edit applications application host-unreachable]
user@host# set icmp-type 5 icmp-code 0
```

2. Set the inactivity timeout value.

```
[edit applications application host-unreachable]
user@host# set inactivity-timeout 4
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show applications** command.

RELATED DOCUMENTATION

Address Books and Address Sets | 44

Custom Policy Applications

IN THIS SECTION

- Understanding Custom Policy Applications | 96
- Custom Application Mappings | 96
- Example: Adding and Modifying Custom Policy Applications | 97
- Example: Configuring Custom Policy Application Term Options | 100

Custom policy application is an alternate feature for predefined policy applications. If you do not want to use predefined policy applications in your policy, you can create custom applications. Junos OS allows you to configure custom applications for your policy.

Understanding Custom Policy Applications

If you do not want to use predefined applications in your policy, you can easily create custom applications.

You can assign each custom application the following attributes:

- Name
- Transport protocol
- Source and destination port numbers for applications using TCP or UDP
- Type and code values for applications using ICMP
- Timeout value

Custom Application Mappings

The application option specifies the Layer 7 application that maps to the Layer 4 application that you reference in a policy. A predefined application already has a mapping to a Layer 7 application. However, for custom applications, you must link the application to a policy explicitly, especially if you want the policy to apply an Application Layer Gateway (ALG) or deep inspection to the custom application.

> **NOTE:** Junos OS supports ALGs for numerous applications, including DNS, FTP, H.323, HTTP, RSH, SIP, Telnet, and TFTP.

Applying an ALG to a custom application involves the following two steps:

- Define a custom application with a name, timeout value, transport protocol, and source and destination ports.
- When configuring a policy, reference that application and the application type for the ALG that you want to apply.

Example: Adding and Modifying Custom Policy Applications

IN THIS SECTION

- Requirements | **97**
- Overview | **97**
- Configuration | **98**
- Verification | **99**

This example shows how to add and modify custom policy applications.

Requirements

Before you begin, create addresses and security zones. See "Example: Creating Security Zones" on page 29.

Overview

In this example, you create a custom application using the following information:

- A name for the application: **cust-telnet**.
- A range of source port numbers: **1** through **65535**.
- A destination port number: 23000.
- The protocol used by the application: TCP.

Once the custom application **cust-telnet** is created the following information is modified:

- The protocol used by the application is modified to : TCP.
- A range of source port numbers: **1** through **51100**.
- A destination port number: 11000.

Configuration

Step-by-Step Procedure

The following example requires you to navigate through various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To add and modify a custom policy application:

1. Configure TCP and specify the source port and destination port.

```
[edit applications application cust-telnet]
user@host# set protocol tcp source-port 65535 destination-port 23000
```

2. Specify the length of time that the application is inactive.

```
[edit applications application cust-telnet]
user@host# set inactivity-timeout 1800
```

3. Modify the custom policy application **cust-telnet** :
   - Delete the source and destination ports configured for TCP.
   - Configure UDP and specify the source port and destination port.
   - Specify the length of time that UDP is inactive.

```
[edit]
user@host# delete applications application cust-telnet source-port
user@host# delete applications application cust-telnet destination-port
user@host# set applications application cust-telnet protocol udp source-port 51100 destination-port 11000
user@host# set inactivity-timeout 1500
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
```

```
user@host# commit
```

Verification

IN THIS SECTION

- Verifying The Modified Custom Policy Application | 99

Verifying The Modified Custom Policy Application

Purpose

To verify if the custom policy application has been modified successfully.

Action

From operational mode, enter the **show applications application *cust-telnet*** command to display the details of the custom policy application - **cust-telnet**.

user@host> show applications application *cust-telnet*

```
protocol udp;
source-port 51100;
destination-port 11000;
inactivity-timeout 1500;
```

NOTE: The timeout value is in seconds. If you do not set it, the timeout value of a custom application is 1800 seconds. If you do not want an application to time out, type **never**.

Meaning

The output displays information about the *cust-telnet* application. Verify the following information:

- Configured policy name.
- Source and destination ports.
- Length of time (in seconds) that the application is inactive.

SEE ALSO

Security Policies Overview | 23

Security Policy Applications Overview | 69

Understanding Custom Policy Applications | 96

Example: Defining a Custom ICMP Application | 93

Example: Configuring Custom Policy Application Term Options

IN THIS SECTION

- Requirements | 100
- Overview | 100
- Configuration | 101
- Verification | 103

This example shows how to configure applications properties and term options for application protocols.

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- A PC

Before you begin:

- Configure the required applications. See “Example: Adding and Modifying Custom Policy Applications” on page 97 .

Overview

In this example, you create an application name, app-name, and a term called custom-options to define your custom policy application term options.

You configure Domain Name Service (DNS) as the Application Layer Gateway (ALG) type and UDP as the networking protocol type. You set the source port to 24000 and the destination port to 23000. Then you set the Internet Control Message Protocol (ICMP) packet type value to 5 and the ICMP code value to 0. You set the remote procedure call (RPC) program number value to 50 and the Universal Unique Identifier (UUID) value to 1be617c0-31a5-11cf-a7d8-00805f48a135. Finally, you set the inactivity-timeout value to 60.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
user@host# set applications application app-name term custom-options
user@host# set applications application app-name term custom-options alg dns
user@host#set applications application app-name term custom-options protocol udp
user@host#set applications application app-name term custom-options source-port 24000
user@host#set applications application app-name term custom-options destination-port 23000
user@host#set applications application app-name term custom-options icmp-type 5
user@host#set applications application app-name term custom-options icmp-code 0
user@host#set applications application app-name term custom-options rpc-program-number 50
user@host#set applications application app-name term custom-options uuid
   1be617c0-31a5-11cf-a7d8-00805f48a135
user@host#set applications application app-name term custom-options inactivity-timeout 60
```

Step-by-Step Procedure

To configure custom policy application term options:

1. Configure the term name.

   ```
   [edit applications]
   user@host# set application app-name term custom-options
   ```

2. Configure the ALG type.

   ```
   [edit applications]
   user@host# set application app-name term custom-options alg dns
   ```

3. Configure the networking protocol type.

```
[edit applications]
user@host# set application app-name term custom-options protocol udp
```

4. Configure the source port number.

```
[edit applications]
user@host#set application app-name term custom-options source-port 24000
```

5. Configure the TCP or UDP destination port number.

```
[edit applications]
user@host# set application app-name term custom-options destination-port 23000
```

6. Specify the application type value.

```
[edit applications]
user@host# set application app-name term custom-options icmp-type 5
```

7. Specify the application code value.

```
[edit applications]
user@host# set application app-name term custom-options icmp-code 0
```

8. Specify the RPC program number.

```
[edit applications]
user@host#  set application app-name term custom-options rpc-program-number 50
```

9. Specify the UUID value.

```
[edit applications]
user@host# set application app-name term custom-options uuid 1be617c0-31a5-11cf-a7d8-00805f48a135
```

10. Specify the inactivity timeout value.

```
[edit applications]
```

```
user@host# set application app-name term custom-options inactivity-timeout 60
```

Results

From configuration mode, confirm your configuration by entering the **show applications** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
   user@host# show applications
   application app-name {
   term custom-options alg dns protocol udp source-port 24000 icmp-type 5 icmp-code 0 rpc-program-number
      50 uuid 1be617c0-31a5-11cf-a7d8-00805f48a135 inactivity-timeout 60;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the Configuration

Purpose

Verify that the configuration is correct.

Action

From operational mode, enter the **show applications** command.

```
user@host> show applications
   application app-name {
   term custom-options alg dns protocol udp source-port 24000 icmp-type 5 icmp-code 0 rpc-program-number
      50 uuid 1be617c0-31a5-11cf-a7d8-00805f48a135 inactivity-timeout 60;
}
```

RELATED DOCUMENTATION

Security Policy Applications and Application Sets | 69

5
CHAPTER

Security Policies

Configuring Security Policies | **105**

Unified Security Policies | **145**

Global Security Policies | **172**

User Role Firewall Security Policies | **182**

Reordering Security Policies | **206**

Scheduling Security Policies | **209**

Configuring Security Policies for a VRF Routing Instance | **215**

Configuring Security Policies Using VRF Group | **246**

Monitoring and Troubleshooting Security Policies | **258**

Configuring Security Policies

IN THIS SECTION

- Understanding Security Policy Elements | 105
- Understanding Security Policy Rules | 106
- Understanding Security Policies for Self Traffic | 110
- Security Policies Configuration Overview | 111
- Best Practices for Defining Policies on SRX Series Devices | 111
- Configuring Policies Using the Firewall Wizard | 115
- Example: Configuring a Security Policy to Permit or Deny All Traffic | 115
- Example: Configuring a Security Policy to Permit or Deny Selected Traffic | 120
- Example: Configuring a Security Policy to Permit or Deny Wildcard Address Traffic | 125
- Example: Configuring a Security Policy to Redirect Traffic Logs to an External System Log Server | 129
- TAP Mode for Security Zones and Policies | 133
- Dynamic Address Groups in Security Policies | 138

To secure a network, a network administrator must create a security policy that outlines all of the network resources within that business and the required security level for those resources. Junos OS allows you to configure security policies. Security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall.

Understanding Security Policy Elements

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service. A policy permits, denies, or tunnels specified types of traffic unidirectionally between two points.

Each policy consists of:

- A unique name for the policy.
- A **from-zone** and a **to-zone**, for example: user@host# **set security policies from-zone untrust to-zone untrust**

- A set of match criteria defining the conditions that must be satisfied to apply the policy rule. The match criteria are based on a source IP address, destination IP address, and applications. The user identity firewall provides greater granularity by including an additional tuple, source-identity, as part of the policy statement.
- A set of actions to be performed in case of a match—permit, deny, or reject.
- Accounting and auditing elements—counting, logging, or structured system logging.

If the SRX Series receives a packet that matches those specifications, it performs the action specified in the policy.

Security policies enforce a set of rules for transit traffic, identifying which traffic can pass through the firewall and the actions taken on the traffic as it passes through the firewall. Actions for traffic matching the specified criteria include permit, deny, reject, log, or count.

For SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices, a factory default security policy is provided that:

- permits all traffic from the trust zone to the untrust zone.
- denies all traffic from the untrust zone to the trust zone.
- allows all traffic from the trust zone to the untrust zone.

Understanding Security Policy Rules

The security policy applies the security rules to the transit traffic within a context (**from-zone** to **to-zone**). Each policy is uniquely identified by its name. The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Each policy is associated with the following characteristics:

- A source zone
- A destination zone
- One or many source address names or address set names
- One or many destination address names or address set names
- One or many application names or application set names

These characteristics are called the *match criteria*. Each policy also has actions associated with it: permit, deny, reject, count, log, and VPN tunnel. You have to specify the match condition arguments when you configure a policy, source address, destination address, and application name.

You can specify to configure a policy with IPv4 or IPv6 addresses using the wildcard entry **any**. When flow support is not enabled for IPv6 traffic, **any** matches IPv4 addresses. When flow support is enabled for IPv6 traffic, **any** matches both IPv4 and IPv6 addresses. To enable flow-based forwarding for IPv6 traffic, use the **set security forwarding-options family inet6 mode flow-based** command. You can also specify the wildcard **any-ipv4** or **any-ipv6** for the source and destination address match criteria to include only IPv4 or only IPv6 addresses, respectively.

When flow support for IPv6 traffic is enabled, the maximum number of IPv4 or IPv6 addresses that you can configure in a security policy is based on the following match criteria:

- Number_of_src_IPv4_addresses + number_of_src_IPv6_addresses * 4 <= 1024
- Number_of_dst_IPv4_addresses + number_of_dst_IPv6_addresses * 4 <= 1024

Thr reason for the match criteria is that an IPv6 address uses four times the memory space that an IPv4 address uses.

> **NOTE:** You can configure a security policy with IPv6 addresses only if flow support for IPv6 traffic is enabled on the device.

If you do not want to specify a specific application, enter **any** as the default application. To look up the default applications, from configuration mode, enter **show groups junos-defaults | find applications (predefined applications)**. For example, if you do not supply an application name, the policy is installed with the application as a wildcard (default). Therefore, any data traffic that matches the rest of the parameters in a given policy would match the policy regardless of the application type of the data traffic.

> **NOTE:** If a policy is configured with multiple applications, and more than one of the applications match the traffic, then the application that best meets the match criteria is selected.

The action of the first policy that the traffic matches is applied to the packet. If there is no matching policy, the packet is dropped. Policies are searched from top to bottom, so it is a good idea to place more specific policies near the top of the list. You should also place IPsec VPN tunnel policies near the top. Place the more general policies, such as one that would allow certain users access to all Internet applications, at the bottom of the list. For example, place deny-all or reject-all policies at the bottom after all of the specific policies have been parsed before and legitimate traffic has been allowed/count/logged.

> **NOTE:** Support for IPv6 addresses is added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) is added in Junos OS Release 10.4.

Policies are looked up during flow processing after firewall filters and screens have been processed and route look up has been completed by the Services Processing Unit (SPU) (for SRX5400, SRX5600, and SRX5800 devices). Policy look up determines the destination zone, destination address, and egress interface.

When you are creating a policy, the following policy rules apply:

- Security policies are configured in a **from-zone** to **to-zone** direction. Under a specific zone direction, each security policy contains a name, match criteria, an action, and miscellaneous options.
- The policy name, match criteria, and action are required.
- The policy name is a keyword.
- The source address in the match criteria is composed of one or more address names or address set names in the **from-zone**.
- The destination address of the match criteria is composed of one or more address names or address set names in the **to-zone**.
- The application name in the match criteria is composed of the name of one or more applications or application sets.
- One of the following actions is required: permit, deny, or reject.
- Accounting and auditing elements can be specified: count and log.
- You can enable logging at the end of a session with the **session-close** command, or at the beginning of the session with the **session-init** command.
- When the count alarm is turned on, specify alarm thresholds in bytes per second or kilobytes per minute.
- You cannot specify **global** as either the **from-zone** or the **to-zone** except under following condition:

  Any policy configured with the **to-zone** as a global zone must have a single destination address to indicate that either static NAT or incoming NAT has been configured in the policy.
- In SRX Series Services Gateways, the policy permit option with NAT is simplified. Each policy will optionally indicate whether it allows NAT translation, does not allow NAT translation, or does not care.
- Address names cannot begin with the following reserved prefixes. These are used only for address NAT configuration:
  - **static_nat_**
  - **incoming_nat_**
  - **junos_**
- Application names cannot begin with the **junos_** reserved prefix.

Understanding Wildcard Addresses

Source and destination addresses are two of the five match criteria that should be configured in a security policy. You can now configure wildcard addresses for the source and destination address match criteria in a security policy. A wildcard address is represented as A.B.C.D/wildcard-mask. The wildcard mask determines which of the bits in the IP address A.B.C.D should be ignored by the security policy match criteria. For example, the source IP address 192.168.0.11/255.255.0.255 in a security policy implies that the security policy match criteria can discard the third octet in the IP address (symbolically represented as 192.168.*.11). Therefore, packets with source IP addresses such as 192.168.1.11 and 192.168.22.11 conform to the match criteria. However, packets with source IP addresses such as 192.168.0.1 and 192.168.1.21 do not satisfy the match criteria.

The wildcard address usage is not restricted to full octets only. You can configure any wildcard address. For example, the wildcard address 192.168. 7.1/255.255.7.255 implies that you need to ignore only the first 5 bits of the third octet of the wildcard address while making the policy match. If the wildcard address usage is restricted to full octets only, then wildcard masks with either 0 or 255 in each of the four octets only will be permitted.

> **NOTE:** The first octet of the wildcard mask should be greater than 128. For example, a wildcard mask represented as 0.255.0.255 or 1.255.0.255 is invalid.

A wildcard security policy is a simple firewall policy that allows you to permit, deny, and reject the traffic trying to cross from one security zone to another. You should not configure security policy rules using wildcard addresses for services such as Unified Threat Management (UTM).

> **NOTE:** Only Intrusion and Prevention (IDP) for IPv6 sessions is supported for all SRX5400, SRX5600, and SRX5800 devices. UTM for IPv6 sessions is not supported. If your current security policy uses rules with the IP address wildcard any, and UTM features are enabled, you will encounter configuration commit errors because UTM features do not yet support IPv6 addresses. To resolve the errors, modify the rule returning the error so that the any-ipv4 wildcard is used; and create separate rules for IPv6 traffic that do not include UTM features.

Configuring wildcard security policies on a device affects performance and memory usage based on the number of wildcard policies configured per from-zone and to-zone context. Therefore, you can only configure a maximum of 480 wildcard policies for a specific from-zone and to-zone context.

SEE ALSO

Understanding Security Policy Ordering | 206

Understanding Security Policies for Self Traffic

Security policies are configured on the devices to apply services to the traffic flowing through the device. For example UAC and UTM policies are configured to apply services to the transient traffic.

Self-traffic or host traffic, is the host-inbound traffic; that is, the traffic terminating on the device or the host-outbound traffic that is the traffic originating from the device. You can now configure policies to apply services on self traffic. Services like the SSL stack service that must terminate the SSL connection from a remote device and perform some processing on that traffic, IDP services on host-inbound traffic, or IPsec encryption on host-outbound traffic must be applied through the security policies configured on self-traffic.

When you configure a security policy for self-traffic, the traffic flowing through the device is first checked against the policy, then against the **host-inbound-traffic** option configured for the interfaces bound to the zone.

You can configure the security policy for self-traffic to apply services to self-traffic. The host-outbound policies will work only in cases where the packet that originated in the host device goes through the flow and the incoming interface of this packet is set to local.

The advantages of using the self-traffic are:

- You can leverage most of the existing policy or flow infrastructure used for the transit traffic.
- You do not need a separate IP address to enable any service.
- You can apply services or policies to any host-inbound traffic with the destination IP address of any interface on the device.

> **NOTE:** You can configure the security policy for self-traffic with relevant services only. For example, it is not relevant to configure the fwauth service on host-outbound traffic, and gprs-gtp services are not relevant to the security policies for self-traffic.

The security policies for the self traffic are configured under the new default security zone called the *junos-host* zone. The junos-host zone will be part of the junos-defaults configuration, so users can delete it. The existing zone configurations such as interfaces, screen, tcp-rst, and host-inbound-traffic options are not meaningful to the junos-host zone. Therefore there is no dedicated configuration for the junos-host zone.

NOTE: You can use host-inbound-traffic to control incoming connections to a device; however it does not restrict traffic going out of the device. Whereas, junos-host-zone allows you to select the application of your choice and also restrict outgoing traffic. For example, services like NAT, IDP, UTM, and so forth can now be enabled for traffic going in or out of the SRX Series device using junos-host-zone.

Security Policies Configuration Overview

You must complete the following tasks to create a security policy:

1. Create zones. See "Example: Creating Security Zones" on page 29.
2. Configure an address book with addresses for the policy. See "Example: Configuring Address Books and Address Sets" on page 53.
3. Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 71.
4. Create the policy. See "Example: Configuring a Security Policy to Permit or Deny All Traffic" on page 115, "Example: Configuring a Security Policy to Permit or Deny Selected Traffic" on page 120, and "Example: Configuring a Security Policy to Permit or Deny Wildcard Address Traffic" on page 125.
5. Create schedulers if you plan to use them for your policies. See "Example: Configuring Schedulers for a Daily Schedule Excluding One Day" on page 211.

The Firewall Policy Wizard enables you to perform basic security policy configuration. For more advanced configuration, use the J-Web interface or the CLI.

SEE ALSO

Troubleshooting Security Policies | 269

Best Practices for Defining Policies on SRX Series Devices

A secure network is vital to a business. To secure a network, a network administrator must create a security policy that outlines all of the network resources within that business and the required security level for those resources. The security policy applies the security rules to the transit traffic within a context

(from-zone to to-zone) and each policy is uniquely identified by its name. The traffic is classified by matching the source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Table 20 on page 112 provides the policy limitations for SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX650, SRX550M, SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices. Platform support depends on the Junos OS release in your installation.

> **NOTE:** Starting with Junos OS Release 12.3X48-D15 and Junos OS Release 17.3R1, the maximum number of address objects per policy for SRX5400, SRX5600, and SRX5800 devices increases from 1024 to 4096, and the maximum number of policies per context increases from 10240 to 80,000.
>
> Starting with Junos OS Release 17.3R1, the number of security policies and the maximum number of policies per context for SRX5400, SRX5600, and SRX5800 devices increases from 80,000 to 100,000.
>
> Starting with Junos OS Release 15.1X49-D120, the number of address objects per policy for SRX5400, SRX5600, and SRX5800 increases from 4096 to 16,000.

Table 20: Policy Limitations for SRX Series Devices

SRX Series Devices	Address objects	Application objects	Security policies	Policy contexts (zone pairs)	Policies per context	Policies with counting enabled
SRX300 SRX320	2048	128	1024	256	1024	256
SRX340	2048	128	2048	512	2048	256
SRX345	2048	128	4096	1024	4096	256
SRX380	2048	128	4096	1024	4096	256
SRX550 SRX650	1024	128	10240	2048	10240	1024
SRX550M	2048	128	10240	2048	10240	1024
SRX1400 SRX1500	1024	3072	16000	4096	16000	1024

Table 20: Policy Limitations for SRX Series Devices *(continued)*

SRX Series Devices	Address objects	Application objects	Security policies	Policy contexts (zone pairs)	Policies per context	Policies with counting enabled
SRX3400 SRX3600	4096	3072	40000	4096	40000	1024
SRX4100	1024	3072	60000	4096	60000	1024
SRX4200	1024	3072	60000	4096	60000	1024
SRX4600	4096	3072	80000	8192	80000	1024
SRX5400 SRX5600 SRX5800	16000	3072	100000	8192	100000	1024

Therefore, as you increase the number of addresses and applications in each rule, the amount of memory that is used by the policy definition increases, and sometimes the system runs out of memory with fewer than 80,000 policies.

To get the actual memory utilization of a policy on the Packet Forwarding Engine (PFE) and the Routing Engine (RE), you need to take various components of the memory tree into consideration. The memory tree includes the following two components:

- Policy context–Used to organize all policies in this context. Policy context includes variables such as source and destination zones.
- Policy entity–Used to hold the policy data. Policy entity calculates memory using parameters such as policy name, IP addresses, address count, applications, firewall authentication, WebAuth, IPsec, count, application services, and Junos Services Framework (JSF).

Additionally, the data structures used to store policies, rule sets, and other components use different memory on the Packet Forwarding Engine and on the Routing Engine. For example, address names for each address in the policy are stored on the Routing Engine, but no memory is allocated at the Packet Forwarding Engine level. Similarly, port ranges are expanded to prefix and mask pairs and are stored on the Packet Forwarding Engine, but no such memory is allocated on the Routing Engine.

Accordingly, depending on the policy configuration, the policy contributors to the Routing Engine are different from those to the Packet Forwarding Engine, and memory is allocated dynamically.

Memory is also consumed by the “deferred delete” state. In the deferred delete state, when an SRX Series device applies a policy change, there is transitory peak usage whereby both the old and new policies are

present. So for a brief period, both old and new policies exist on the Packet Forwarding Engine, taking up twice the memory requirements.

Therefore, there is no definitive way to infer clearly how much memory is used by either component (Packet Forwarding Engine or Routing Engine) at any given point in time, because memory requirements are dependent on specific configurations of policies, and memory is allocated dynamically.

The following best practices for policy implementation enable you to better use system memory and to optimize policy configuration:

- Use single prefixes for source and destination addresses. For example, instead of using /32 addresses and adding each address separately, use a large subnet that covers most of the IP addresses you require.
- Use application “any” whenever possible. Each time you define an individual application in the policy, you can use an additional 52 bytes.
- Use fewer IPv6 addresses because IPv6 addresses consume more memory.
- Use fewer zone pairs in policy configurations. Each source or destination zone uses about 16,048 bytes of memory.
- The following parameters can change how memory is consumed by the bytes as specified:
  - Firewall authentication–About 16 bytes or more (unfixed)
  - Web authentication–About 16 bytes or more (unfixed)
  - IPsec–12 bytes
  - Application services–28 bytes
  - Count–64 bytes
- Check memory utilization before and after compiling policies.

> **NOTE:** The memory requirement for each device is different. Some devices support 512,000 sessions by default, and the bootup memory is usually at 72 to 73 percent. Other devices can have up to 1 million sessions and the bootup memory can be up to 83 to 84 percent. In the worst-case scenario, to support about 80,000 policies in the SPU, the SPU should boot with a flowd kernel memory consumption of up to 82 percent, and with at least 170 megabytes of memory available.

SEE ALSO

Understanding Global Address Books | 46

Global Policy Overview | 172

Checking Memory Usage on SRX Series Devices | 264

Configuring Policies Using the Firewall Wizard

The Firewall Policy Wizard enables you to perform basic security policy configuration on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices.. For more advanced configuration, use the J-Web interface or the CLI.

To configure policies using the Firewall Policy Wizard:

1. Select **Configure>Tasks>Configure FW Policy** in the J-Web interface.

2. Click the Launch Firewall Policy Wizard button to launch the wizard.

3. Follow the prompts in the wizard.

The upper-left area of the wizard page shows where you are in the configuration process. The lower-left area of the page shows field-sensitive help. When you click a link under the Resources heading, the document opens in your browser. If the document opens in a new tab, be sure to close only the tab (not the browser window) when you close the document.

Example: Configuring a Security Policy to Permit or Deny All Traffic

IN THIS SECTION

- Requirements | 116
- Overview | 116
- Configuration | 117
- Verification | 119

This example shows how to configure a security policy to permit or deny all traffic.

Requirements

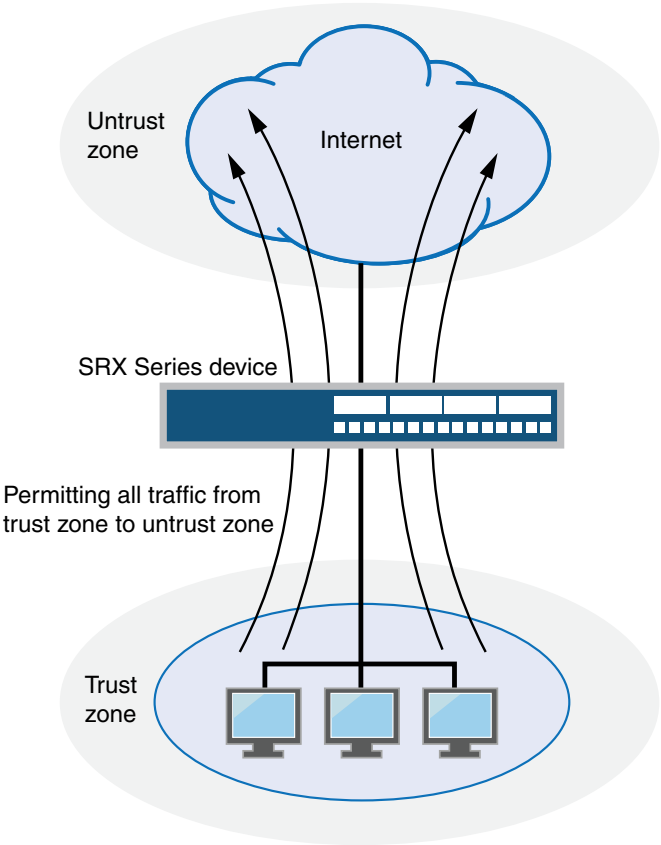
Before you begin:

- Create zones. See “Example: Creating Security Zones” on page 29.
- Configure an address book and create addresses for use in the policy. See “Example: Configuring Address Books and Address Sets” on page 53.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See “Example: Configuring Security Policy Applications and Application Sets” on page 71.

Overview

In the Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on traffic as it passes through the device. From the perspective of security policies, the traffic enters one security zone and exits another security zone. In this example, you configure the trust and untrust interfaces, ge-0/0/2 and ge-0/0/1. See Figure 4 on page 116.

Figure 4: Permitting All Traffic



This configuration example shows how to:

- Permit or deny all traffic from the trust zone to the untrust zone but block everything from the untrust zone to the trust zone.
- Permit or deny selected traffic from a host in the trust zone to a server in the untrust zone at a particular time.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
set security policies from-zone trust to-zone untrust policy permit-all match source-address any
set security policies from-zone trust to-zone untrust policy permit-all match destination-address any
set security policies from-zone trust to-zone untrust policy permit-all match application any
set security policies from-zone trust to-zone untrust policy permit-all then permit
set security policies from-zone untrust to-zone trust policy deny-all match source-address any
set security policies from-zone untrust to-zone trust policy deny-all match destination-address any
set security policies from-zone untrust to-zone trust policy deny-all match application any
set security policies from-zone untrust to-zone trust policy deny-all then deny
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a security policy to permit or deny all traffic:

1. Configure the interfaces and security zones.

```
[edit security zones]
user@host# set security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
user@host# set security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
```

2. Create the security policy to permit traffic from the trust zone to the untrust zone.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy permit-all match source-address any
user@host# set policy permit-all match destination-address any
```

```
user@host# set policy permit-all match application any
user@host# set policy permit-all then permit
```

3. Create the security policy to deny traffic from the untrust zone to the trust zone.

```
[edit security policies from-zone untrust to-zone trust]
user@host# set policy deny-all match source-address any
user@host# set policy deny-all match destination-address any
user@host# set policy deny-all match application any
user@host# set policy deny-all then deny
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

NOTE: The configuration example is a default permit-all from the trust zone to the untrust zone.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy permit-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy deny-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
```

```
        then {
            deny;
        }
    }
}
```

```
user@host# show security zones
security-zone trust {
    interfaces {
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
        }
    }
}
security-zone untrust {
    interfaces {
        ge-0/0/1.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies detail** command to display a summary of all security policies configured on the device.

Meaning

The output displays information about policies configured on the system. Verify the following information:

- From and to zones
- Source and destination addresses
- Match criteria

Example: Configuring a Security Policy to Permit or Deny Selected Traffic

IN THIS SECTION

- Requirements | 120
- Overview | 120
- Configuration | 121
- Verification | 124

This example shows how to configure a security policy to permit or deny selected traffic.

Requirements

Before you begin:

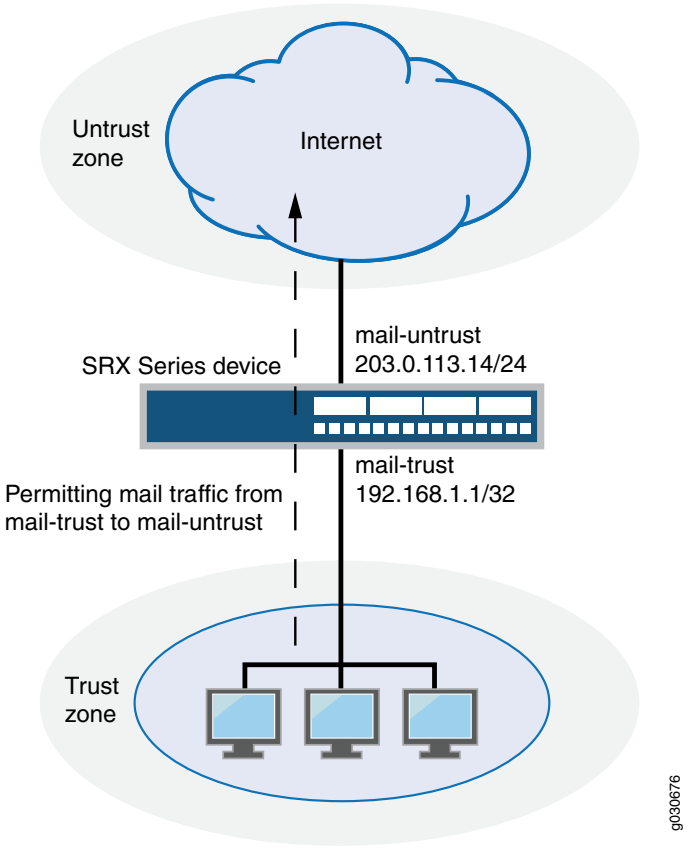
- Create zones. See “Example: Creating Security Zones” on page 29.
- Configure an address book and create addresses for use in the policy. See “Example: Configuring Address Books and Address Sets” on page 53.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See “Example: Configuring Security Policy Applications and Application Sets” on page 71.
- Permit traffic to and from trust and untrust zones. See “Example: Configuring a Security Policy to Permit or Deny All Traffic” on page 115.

Overview

In Junos OS, security policies enforce rules for the transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on the traffic as it passes through the device. From the perspective of security policies, the traffic enters one security zone and exits another security zone. In

this example, you configure a specific security policy to allow only e-mail traffic from a host in the trust zone to a server in the untrust zone. No other traffic is allowed. See Figure 5 on page 121.

Figure 5: Permitting Selected Traffic



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
set security address-book book1 address mail-untrust 203.0.113.14/24
set security address-book book1 attach zone untrust
set security address-book book2 address mail-trust 192.168.1.1/32
set security address-book book2 attach zone trust
```

```
set security policies from-zone trust to-zone untrust policy permit-mail match source-address mail-trust
set security policies from-zone trust to-zone untrust policy permit-mail match destination-address mail-untrust
set security policies from-zone trust to-zone untrust policy permit-mail match application junos-mail
set security policies from-zone trust to-zone untrust policy permit-mail then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a security policy to allow selected traffic:

1. Configure the interfaces and security zones.

```
[edit security zones]
user@host# set security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
user@host# set security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
```

2. Create address book entries for both the client and the server. Also, attach security zones to the address books.

```
[edit security address-book book1]
user@host# set address mail-untrust 203.0.113.14/24
user@host# set attach zone untrust
```

```
[edit security address-book book2]
user@host# set address mail-trust 192.168.1.1/32
user@host# set attach zone trust
```

3. Define the policy to permit mail traffic.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy permit-mail match source-address mail-trust
user@host# set policy permit-mail match destination-address mail-untrust
user@host# set policy permit-mail match application junos-mail
user@host# set policy permit-mail then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy permit-mail {
        match {
            source-address mail-trust;
            destination-address mail-untrust;
            application junos-mail;
        }
        then {
            permit;
        }
    }
}
```

```
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        interfaces {
            ge-0/0/2 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/1 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
```

```
user@host# show security address-book
book1 {
    address mail-untrust 203.0.113.14/24;
    attach {
        zone untrust;
    }
}
    book2 {
        address mail-trust 192.168.1.1/32;
        attach {
            zone trust;
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies detail** command to display a summary of all security policies configured on the device.

Meaning

The output displays information about policies configured on the system. Verify the following information:

- From and to zones
- Source and destination addresses
- Match criteria

Example: Configuring a Security Policy to Permit or Deny Wildcard Address Traffic

IN THIS SECTION

- Requirements | 125
- Overview | 125
- Configuration | 126
- Verification | 128

This example shows how to configure a security policy to permit or deny wildcard address traffic.

Requirements

Before you begin:

- Understand wildcard addresses. See "Understanding Security Policy Rules" on page 106.
- Create zones. See "Example: Creating Security Zones" on page 29.
- Configure an address book and create addresses for use in the policy. See "Example: Configuring Address Books and Address Sets" on page 53.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 71.
- Permit traffic to and from trust and untrust zones. See "Example: Configuring a Security Policy to Permit or Deny All Traffic" on page 115.
- Permit e-mail traffic to and from trust and untrust zones. See "Example: Configuring a Security Policy to Permit or Deny Selected Traffic" on page 120

Overview

In the Junos operating system (Junos OS), security policies enforce rules for the transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on the traffic as it passes through the device. From the perspective of security policies, the traffic enters one security zone and exits another security zone. In this example, you configure a specific security to allow only wildcard address traffic from a host in the trust zone to the untrust zone. No other traffic is allowed.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** in configuration mode.

```
set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
set security address-book book1 address wildcard-trust wildcard-address 192.168.0.11/255.255.0.255
set security address-book book1 attach zone trust
set security policies from-zone trust to-zone untrust policy permit-wildcard match source-address wildcard-trust
set security policies from-zone trust to-zone untrust policy permit-wildcard match destination-address any
set security policies from-zone trust to-zone untrust policy permit-wildcard match application any
set security policies from-zone trust to-zone untrust policy permit-wildcard then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a security policy to allow selected traffic:

1. Configure the interfaces and security zones.

```
[edit security zones]
user@host# set security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
user@host# set security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services all
```

2. Create an address book entry for the host and attach the address book to a zone.

```
[edit security address-book book1]
user@host# set address wildcard-trust wildcard-address 192.168.0.11/255.255.0.255
user@host# set attach zone trust
```

3. Define the policy to permit wildcard address traffic.

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy permit-wildcard match source-address wildcard-trust
user@host# set policy permit-wildcard match destination-address any
user@host# set policy permit-wildcard match application any
user@host# set policy permit-wildcard then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy permit-wildcard {
        match {
            source-address wildcard-trust;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

```
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        interfaces {
            ge-0/0/2 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
}
    security-zone untrust {
        interfaces {
            ge-0/0/1 {
                host-inbound-traffic {
                    system-services {
                        all;
```

```
            }
          }
        }
      }
    }
user@host# show security address-book
book1 {
    address wildcard-trust {
        wildcard-address 192.168.0.11/255.255.0.255;
    }
    attach {
        zone trust;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies policy-name permit-wildcard detail** command to display details about the permit-wildcard security policy configured on the device.

Meaning

The output displays information about the permit-wildcard policy configured on the system. Verify the following information:

- From and To zones
- Source and destination addresses
- Match criteria

Example: Configuring a Security Policy to Redirect Traffic Logs to an External System Log Server

IN THIS SECTION

- Requirements | 129
- Overview | 129
- Configuration | 130
- Verification | 132

This example shows how to configure a security policy to send traffic logs generated on the device to an external system log server.

Requirements

This example uses the following hardware and software components:

- A client connected to an SRX5600 device at the interface ge-4/0/5
- A server connected to the SRX5600 device at the interface ge-4/0/1

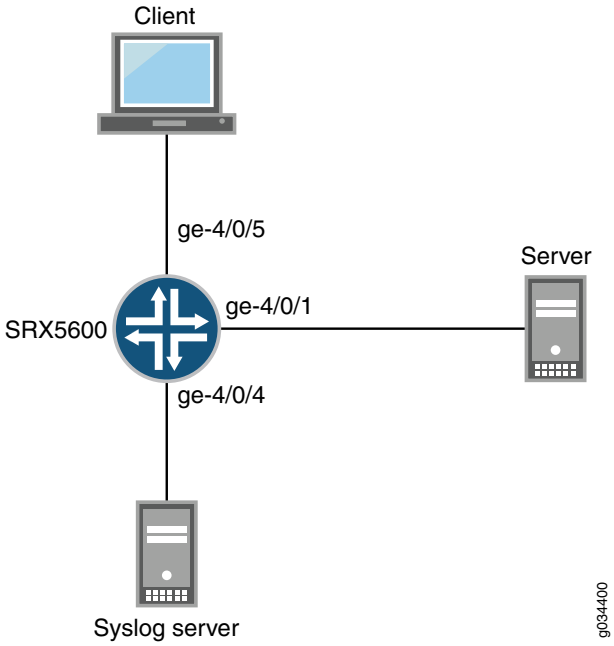
  The logs generated on the SRX5600 device are stored in a Linux-based system log server.
- An SRX5600 device connected to the Linux-based server at interface ge-4/0/4

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you configure a security policy on the SRX5600 device to send traffic logs, generated by the device during data transmission, to a Linux-based server. Traffic logs record details of every session.

The logs are generated during session establishment and termination between the source and the destination device that are connected to the SRX5600 device.



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** in configuration mode.

```
set security log source-address 127.0.0.1
set security log stream trafficlogs severity debug
set security log stream trafficlogs host 203.0.113.2
set security zones security-zone client host-inbound-traffic system-services all
set security zones security-zone client host-inbound-traffic protocols all
set security zones security-zone client interfaces ge-4/0/5.0
set security zones security-zone server host-inbound-traffic system-services all
set security zones security-zone server interfaces ge-4/0/4.0
set security zones security-zone server interfaces ge-4/0/1.0
set security policies from-zone client to-zone server policy match source-address any
set security policies from-zone client to-zone server policy match destination-address any
set security policies from-zone client to-zone server policy match application any
```

```
set security policies from-zone client to-zone server policy match then permit
set security policies from-zone client to-zone server policy match then log session-init
set security policies from-zone client to-zone server policy match then log session-close
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a security policy to send traffic logs to an external system log server:

1. Configure security logs to transfer traffic logs generated at the SRX5600 device to an external system log server with the IP address 203.0.113.2. The IP address 127.0.0.1 is the loopback address of the SRX5600 device.

   ```
   [edit security log]
   user@host# set source-address 127.0.0.1
   user@host# set stream trafficlogs severity debug
   user@host# set stream trafficlogs host 203.0.113.2
   ```

2. Configure a security zone and specify the types of traffic and protocols that are allowed on interface ge-4/0/5.0 of the SRX5600 device.

   ```
   [edit security zones]
   user@host# set security-zone client host-inbound-traffic system-services all
   user@host# set security-zone client host-inbound-traffic protocols all
   user@host# set security-zone client interfaces ge-4/0/5.0
   ```

3. Configure another security zone and specify the types of traffic that are allowed on the interfaces ge-4/0/4.0 and ge-4/0/1.0 of the SRX5600 device.

   ```
   [edit security zones]
   user@host# set security-zone server host-inbound-traffic system-services all
   user@host# set security-zone server interfaces ge-4/0/4.0
   user@host# set security-zone server interfaces ge-4/0/1.0
   ```

4. Create a policy and specify the match criteria for that policy. The match criteria specifies that the device can allow traffic from any source, to any destination, and on any application.

   ```
   [edit security policies from-zone client to-zone server]
   user@host# set policy match source-address any
   ```

```
user@host# set policy match destination-address any
user@host# set policy match application any
user@host# set policy match then permit any
```

5. Enable the policy to log traffic details at the beginning and at the end of the session.

```
[edit security policies from-zone client to-zone server]
user@host# set policy match then log session-init
user@host# set policy match then log session-close
```

Results

From configuration mode, confirm your configuration by entering the **show security log** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security log
format syslog;
source-address 127.0.0.1;
stream trafficlogs {
    severity debug;
    host {
        203.0.113.2;
    }
}
```

If you are done configuring the device, enter **commit** from the configuration mode.

Verification

IN THIS SECTION

- Verifying Zones | **133**
- Verifying Policies | **133**

Confirm that the configuration is working properly.

Verifying Zones

Purpose

Verify that the security zone is enabled or not.

Action

From operational mode, enter the **show security zones** command.

Verifying Policies

Purpose

Verify that the policy is working.

Action

From operational mode, enter the **show security policies** command on all the devices.

TAP Mode for Security Zones and Policies

IN THIS SECTION

- Understanding TAP Mode Support for Security Zones and Policies | **133**
- Example: Configuring Security Zones and Policies in TAP mode | **134**

The Terminal Access Point (TAP) mode for security zones and policy allows you to passively monitor traffic flows across a network by way of a switch SPAN or mirror port.

Understanding TAP Mode Support for Security Zones and Policies

The Terminal Access Point (TAP) mode is a standby device, which checks the mirrored traffic through switch. If security zones and policies are configured, then the TAP mode inspects the incoming and outgoing traffic by configuring the TAP interface and generating a security log report to display the number of threats detected and the user usage. If some packet gets lost in the tap interface, the security zones and policies terminates the connection, as a result no report generates for this connection. The security zone and policy configuration remains the same as non-TAP mode.

When you configure an SRX Series device to operate in TAP mode, the device generates security log information to display the information on threats detected, application usage, and user details. When the device is configured to operate in TAP mode, the SRX Series device receives packets only from the configured TAP interface. Except the configured TAP interface, other interface are configured to normal

interface that is used as management interface or connected to the outside server. The SRX Series device will generate security report or log according to the incoming traffic.

The security zone and default security policy will be configured after TAP interface is configured. You can configure other zones or policies if required. If one interface is used to connect a server then the IP address, routing-interface, and security configuration also need be configured.

NOTE: You can configure only one TAP interface when you operate the device in TAP mode.

Example: Configuring Security Zones and Policies in TAP mode

IN THIS SECTION

- Requirements | 134
- Overview | 134
- Configuration | 135
- Verification | 136

This example shows how to configure security zones, and policies when the SRX device is configured in TAP (Terminal Access Point) mode.

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- Junos OS Release 19.1R1

Before you begin:

- Read the "Understanding TAP Mode Support for Security Zones and Policies" on page 133 to understand how and where this procedure fits in the overall support for Security Zones and Policies.

Overview

In this example, you configure the SRX Series device to operate in TAP mode. When you configure the SRX Series device to operate in TAP mode, the device generates security log information to display the information on threats detected, application usage, and user details.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter commit from configuration mode.

```
set security zones security-zone tap-zone interfaces ge-0/0/0.0
set security zones security-zone tap-zone application-tracking
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match source-address any
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match destination -address any
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match application any
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then permit
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-init
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-close
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the Junos OS CLI User Guide.

To configure zones in TAP mode:

1. Configure security zone tap-zone interface.

   ```
   user@host# set security zones security-zone tap-zone interfaces ge-0/0/0.0
   ```

2. Configure security zone tap-zone application-tracking.

   ```
   user@host# set security zones security-zone tap-zone application-tracking
   ```

3. Configure security policy that permits traffic from zone tap-zone to zone tap-zone policy tap and configure the match condition.

   ```
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match source-address
     any
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match destination
     -address any
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy match application
     any
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then permit
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-init
   user@host# set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-close
   ```

Results

From configuration mode, confirm your configuration by entering the **show security zones** and **show security policies** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host#show security zones
   security-zone tap-zone {
      interfaces {
         ge-0/0/0.0;
      }
      application-tracking;
   }
[edit]
user@host#show security policies
   from-zone tap-zone to-zone tap-zone {
      policy tap-policy {
         match {
            source-address any;
            destination-address any;
            application any;
         }
         then {
            permit;
            log {
               session-init;
               session-close;
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Policy Configuration in TAP Mode | **137**

To confirm that the configuration is working properly, perform these tasks:

Verifying Policy Configuration in TAP Mode

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies detail** command.

```
user@host> show security policies detail
```

```
node0:
--------------------------------------------------------------------------
Default policy: permit-all
Pre ID default policy: permit-all
Policy: Trust_to_Untrust, action-type: permit, State: enabled, Index: 4, Scope
Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: izone, To zone: ozone
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Session log: at-create, at-close
Policy: Untrust_to_Trust, action-type: permit, State: enabled, Index: 5, Scope
Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: ozone, To zone: izone
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
```

```
    Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
```

Meaning

Displays a summary of all security policies configured on the device in TAP mode.

Dynamic Address Groups in Security Policies

Manually adding address entries into a policy can be time consuming. There are external sources that provide lists of IP addresses that have a specific purpose (such as a blacklist) or that have a common attribute (such as a particular location or behavior that might pose a threat). You can use the external source to identify threat sources by their IP address, then group those addresses into a dynamic address entry, and reference that entry in a security policy. Thereby you can control the traffic to and from those addresses. Each such group of IP addresses is referred to as a dynamic address entry.

The following types of IP addresses are supported:

- Single IP. For example : 192.0.2.0
- IP range. For example : 192.0.2.0- 192.0.2.10
- CIDR. For example : 192.0.2.0/24

Each entry occupies one line. Starting in Junos OS Release 19.3R1, IP address ranges do not need to be sorted in ascending order and the value of the IP entries can overlap in the same feed file. In Junos OS Releases before 19.3R1, IP address ranges need to be sorted in ascending order and the value of the IP entries cannot overlap in the same feed file.

> **NOTE:** A dynamic address entry is a group of IP addresses, not a single IP prefix. A dynamic address entry is different from the security address concepts of address books and address entry addresses.

The following are the benefits of deploying dynamic address entries in security policies:

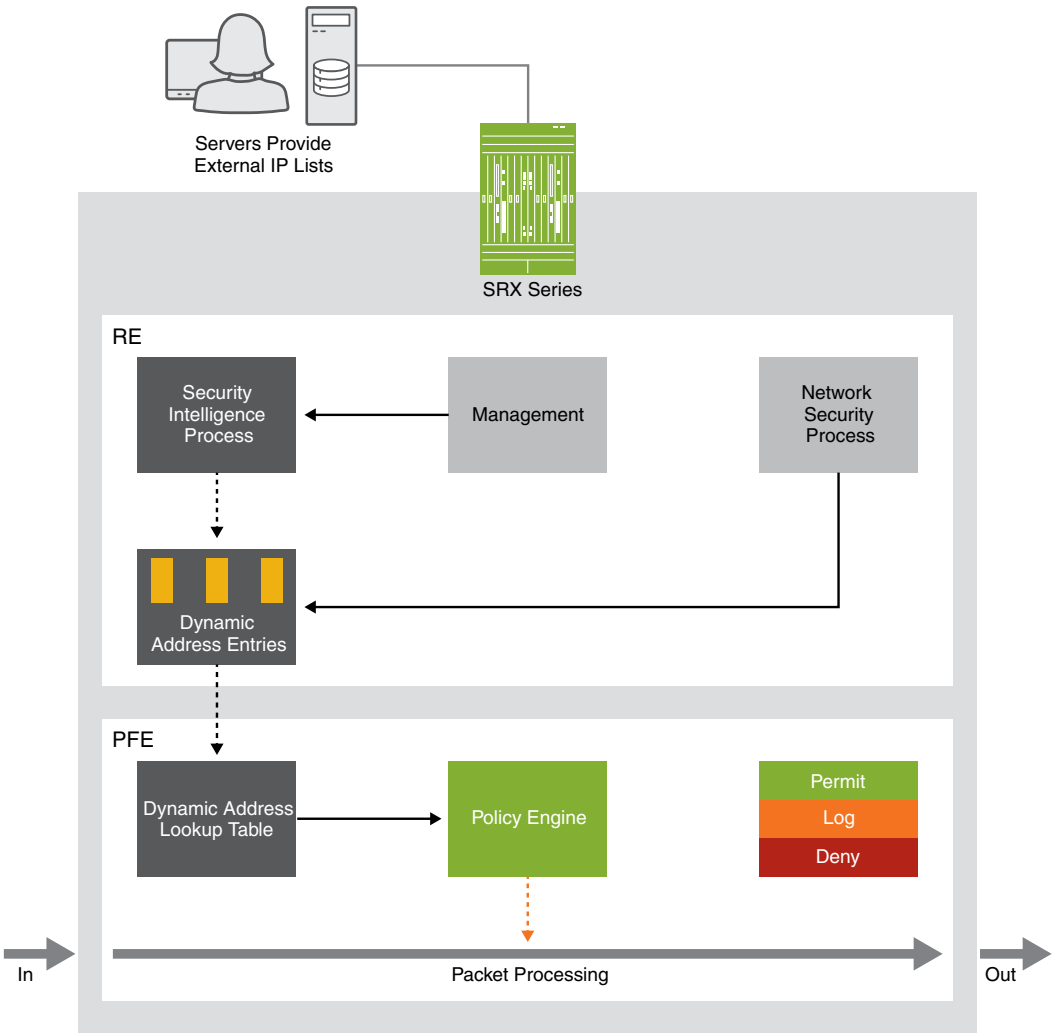
- The network administrator has more control over the traffic to and from groups of IP addresses.
- The external server provides updated IP address feeds to the SRX Series device.
- The administrator's efforts are dramatically reduced. For example, in a legacy security policy configuration, adding 1000 address entries for a policy to reference would require some 2000 lines of configuration.

By defining a dynamic address entry and referencing it in a security policy, up to millions of entries could flow into the SRX Series device without much additional configuration effort.

- No commit process is required to add new addresses. Adding thousands of addresses to a configuration through a legacy method takes a long time to commit. Alternatively, IP addresses in a dynamic address entry come from an external feed, so no commit process is required when the addresses in an entry change.

Figure 6 on page 139 illustrates a functional overview of how the dynamic address entry in a security policy works.

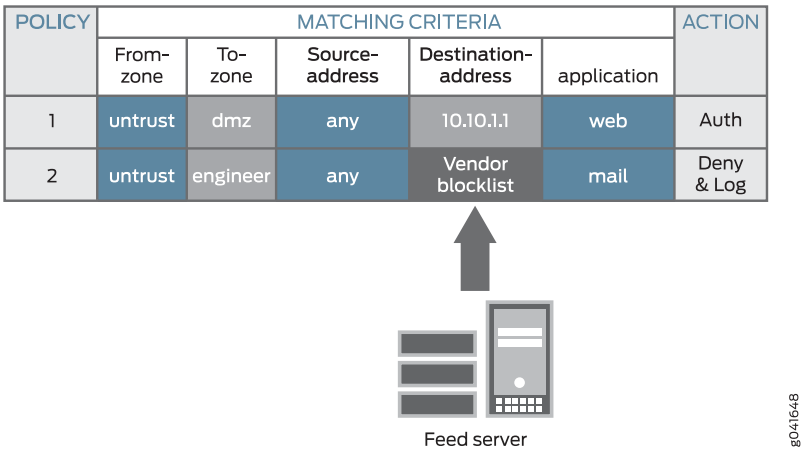
Figure 6: Functional Components of the Dynamic Address Entry in a Security Policy



A security policy references the dynamic address entry in a source address or destination address field (in much the same way that a security policy references a legacy address entry).

Figure 7 on page 140 illustrates a policy that uses a dynamic address entry in the Destination-address field.

Figure 7: A Dynamic Address Entry in a Security Policy



In Figure 7 on page 140, Policy 1 uses the destination address 10.10.1.1, which is a legacy security address entry. Policy 2 uses the destination address Vendor blocklist, which is a dynamic address entry named by the network administrator. Its content is the list of IP addresses retrieved from an external feed file. Packets that match all five criteria (the From-zone named untrust, the To-zone named engineer, any source address, a destination IP address that belongs to the Vendor blocklist dynamic address entry, and the mail application) are handled according to the policy actions, which are to deny and log the packet.

> **NOTE:** The dynamic address entry names share the same name space as legacy security address entries, so do not use the same name for more than one entry. The Junos OS commit process checks that names are not duplicated to avoid a conflict.

Dynamic address groups support the following data feeds:

- Custom lists (whitelists and blacklists)
- GeoIP
- Feed Servers

Bundle Feeds

IN THIS SECTION

- Archive Mode | 141
- Flat File Mode | 142

IP addresses, IP prefixes or IP ranges contained in a dynamic address entry can be updated periodically by downloading an external feed. SRX Series devices periodically initiate a connection to the feed server to download and update the IP lists which contain the updated dynamic addresses.

Starting in Junos OS Release 19.3R1, you can download a single tgz file from server and extract it into multiple children feed files. Each individual file corresponds to one feed. Let individual dynamic-addresses reference the feed inside the bundle file. The bundle file reduces the CPU overhead when too many feeds are configured, where multiple child feeds are compressed into one *.tgz* file

The following bundle feed modes are supported:

Archive Mode

In the archive mode, you need to compress all feed files for the SRX Series device into one tgz file. The SRX Series device downloads this file and extract all the feeds after extraction. This process is explained below:

- When the feed server's url is a url of a file with the suffix *.tgz* instead of original url of folder, this means this server uses a single file to carry all its feeds for SRX Series dynamic-address deployment. In this case, feeds under this server inherit the update-interval or hold-interval from the server. Any user configuration of the update-interval or hold-interval for this feed is ignored.
- After this change, follow the steps below to maintain server feeds as below example.

  The example below shows the steps required to maintain the server feeds:

  1. Place all feed files for the SRX Series device under the folder *feeds-4-srx*
  2. Generate all feed files fd1 fd2 fd3 ..fdN in the folder *feeds-4-srx*
  3. Add or remove the IP ranges from the feeds
  4. Access the files by running the following command: **cd feeds-4-srx;tar -zcvf ../feeds-4-srx.tgz *;cd-**

- Post Step 4, the file *feeds-4-srx.tgz* is ready for download on the SRX Series device containing the same folder which contains the *feeds-4-srx.tgz* file. After the download, the extracted files are placed in the same folder as *feeds-4-srx.tgz*. The following example shows a samle configuration on an SRX Series device:

  [edit]
  set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-srx.tgz
  set security dynamic-address feed-server server-4-srx feed-name feed1 path fd1
  set security dynamic-address feed-server server-4-srx feed-name feed2 path.fd2
  set security dynamic-address feed-server server-4-srx feed-name feed3 path fdN

The *path* parameter requires the relative path of the feed inside the bundle archive.

- If the *tar -zxf feeds-4-srx.tgz* file generates a folder *feeds-4-srx* and this folder holds the feed file *fd1*, then use the following command to configure the feed:

  [edit]

  set security dynamic-address feed-server server-4-srx feed fd1 path feeds-4-srx/fd1

- If the *tar -zxf feeds-4-srx.tgz* file extracts the file *fd1* directly, then use the following command to configure the feed:

  [edit]

  set security dynamic-address feed-server server-4-srx feed fd1 path fd1

Flat File Mode

Flat file mode offers ultimate simplicity for user by introducing one syntax change in existing feed file format. The content of all the feed files are compiled into a single file, with *.bundle* as a suffix. This allows you to manage a single file. The SRX Series device classifies IP ranges in this bundle file into numerous feed files. You can gzip this file as *.bundle.gz* if you can save some bandwidth for transmission. In addition to file format defined earlier, an upper case tag *FEED:* followed by the feed name is introduced. The lines below this tag are regarded as IP ranges belonging to the feed. An example of the file format looks is given below:

root>cat feeds-4-srx.bundle

FEED:fd1

12.1.1.1-12.1.1.2

11.1.1.1-11.1.1.2

FEED:fd2

14.1.1.1-14.1.1.2

The configuration on an SRX Series device is similar to archive mode and is given below:

[edit]

set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-srx.bundle

set security dynamic-address feed-server server-4-srx feed-name fd1 path fd1

set security dynamic-address feed-server server-4-srx feed-name fd2 path fd2

The difference between flat mode and archive mode is the file's suffix and the layout inside the file. You can select the mode that is most convenient for you.

As the feed files are in the plaintext format, gzip can reduce the file size. If a server and an SRX Series device has WAN link in between, use a smaller sized file to be transmitted on the network, in this case, gzip the bundle file and configure the following commands:

[edit]

set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-srx.bundle.gz

set security dynamic-address feed-server server-4-srx feed-name fd1 path fd1

set security dynamic-address feed-server server-4-srx feed-name fd2 path fd2

SEE ALSO

url

Feed Server Support for SRX Series Devices

Table 21:

Platform	Maximum Number of Feed Servers	Maximum Number of Feeds	Maximum Number of Dynamic Addresses entries
SRX300 SRX320 SRX340 SRX345 SRX550 SRX550M SRX650	10	500	500
SRX4100 SRX4200 SRX4600 SRX5400 SRX5600 SRX5800 vSRX vSRX 3.0	100	5000	5000

Table 21: *(continued)*

SRX1500	40	2000	2000

Release History Table

Release	Description
17.3R1	Starting with Junos OS Release 17.3R1, the number of security policies and the maximum number of policies per context for SRX5400, SRX5600, and SRX5800 devices increases from 80,000 to 100,000.
15.1X49-D120	Starting with Junos OS Release 15.1X49-D120, the number of address objects per policy for SRX5400, SRX5600, and SRX5800 increases from 4096 to 16,000.
12.3X48-D15	Starting with Junos OS Release 12.3X48-D15 and Junos OS Release 17.3R1, the maximum number of address objects per policy for SRX5400, SRX5600, and SRX5800 devices increases from 1024 to 4096, and the maximum number of policies per context increases from 10240 to 80,000.
10.4	Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) is added in Junos OS Release 10.4.
10.2	Support for IPv6 addresses is added in Junos OS Release 10.2.

RELATED DOCUMENTATION

Security Zones | **27**

Global Security Policies | **172**

User Role Firewall Security Policies | **182**

Unified Security Policies

IN THIS SECTION

- Unified Policies Overview | 145
- Unified Policies Configuration Overview | 146
- Example: Configure a Unified Policy Using a Redirect Message Profile | 154
- Configure a URL Category with Unified Policies | 160
- Configure Applications in Unified Policies | 165
- Configure Micro-Applications in Unified Policies | 170

Unified policies are the security policies that enable you to use dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time.

Unified Policies Overview

Starting in Junos OS Release 18.2R1, unified policies are supported on SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications within the security policy.

Unified policies are the security policies that enable you to use dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall) match conditions to detect application changes over time. If the traffic matches the security policy rule, one or more actions defined in the policy are applied to the traffic.

By adding dynamic applications to the match criteria, the data traffic is classified based on the Layer 7 application inspection results. AppID identifies dynamic or real-time Layer 4 through Layer 7 applications. After a particular application is identified and the matching policy is found, then the actions are applied according to the policy.

Configuring dynamic applications as match criteria in a security policy is not mandatory.

Examples of configuring dynamic applications as a match condition within a security policy are as follows:

- **set security policies from-zone z1 to-zone z2 policy p1 match dynamic-application junos:FTP**
- **set security policies from-zone z1 to-zone z2 policy p1 match dynamic-application junos:HTTP**

- **set security policies from-zone z1 to-zone z2 policy p1 match dynamic-application junos:GOOGLE**

Examples of configuring dynamic application groups as a match condition within a security policy are as follows:

- **set security policies from-zone trust to-zone untrust policy p1 match dynamic-application junos:p2p**
- **set security policies from-zone trust to-zone untrust policy p1 match dynamic-application junos:web:shopping**

Benefits

- Simplifies application-based security policy management at Layer 7.
- Enables your device to adapt to the dynamic traffic changes in the network.
- Provides greater control and extensibility to manage dynamic applications traffic than a traditional security policy.

Unified Policies Configuration Overview

IN THIS SECTION

- Dynamic Application Configuration Options | **147**
- Default Ports and Protocols as Application Matching Criteria | **147**
- Default Policy Actions Prior to Dynamic Application Identification | **148**
- Global Policy Utilization with Unified Policies | **149**
- Unified Policy Actions | **149**
- Redirect Profile for Reject Action | **149**
- SSL Proxy Profile for Reject Action | **150**
- Match Criteria and Rules for Unified Policies | **151**
- Limitations to Configuring Unified Policies | **153**

The following sections provide more information on unified policies:

Dynamic Application Configuration Options

Table 22 on page 147 provides options for configuring a unified policy with dynamic applications.

Table 22: Dynamic Application Configuration Options

Dynamic Application Configuration Options	Description
Dynamic Applications or Application Groups	Specify dynamic applications or a dynamic application group. Examples are as follows: • **junos:FTP** (dynamic application) • **junos:web:shopping** (dynamic application group)
Any	Configuring the dynamic application as **any** installs the policy with the application as a wildcard (default). If an application cannot be specified, configure **any** as the default application. Data traffic that match the parameters in a unified policy matches the policy regardless of the application type.
None	Configuring the dynamic application as **none** ignores classification results from AppID and does not use the dynamic application in security policy lookups. Within the list of potential match policies, if there is any policy configured with a dynamic application as **none**, this policy is matched as the final policy and is terminal. If any Layer 7 services are configured in this policy, deep packet inspection for the traffic is performed. When upgrading the Junos OS release (where dynamic applications were not supported), all existing traditional policies are considered to be policies with the dynamic application configured as **none**.
Dynamic Application Not Configured	If a dynamic application is not configured within a security policy, the policy is considered to be a traditional security policy This policy is similar to a policy with the dynamic application configured as **none**.

Default Ports and Protocols as Application Matching Criteria

Starting in Junos OS Release 18.2R1, the **junos-defaults** option is introduced in the security policy configuration as application match criteria. The **junos-defaults** group contains preconfigured statements that include predefined values for common applications. As the default protocols and ports are inherited from **junos-defaults**, there is no requirement to explicitly configure the ports and protocols, thus simplifying the security policy configuration.

In the following example, the security policy L7-test-policy uses **junos:HTTP** as the dynamic application and inherits destination TCP ports: 80, 3128, 8000, and 8080 as the application match criteria.

set security policies from-zone trust to-zone untrust policy L7-test-policy match application junos-defaults dynamic-application junos:HTTP

If the application does not have default ports and protocols, then the application uses the default ports and protocols of the dependent application. For example, junos:FACEBOOK-CHAT uses default protocols and ports of HTTP2, HTTPS, and SPDY.

The **junos-defaults** option must be configured along with a dynamic application. If you configure the **junos-defaults** option without specifying any dynamic application, then an error message displays and the configuration commit fails. Use the **show security policies detail** command to validate the **junos-defaults** option.

Default Policy Actions Prior to Dynamic Application Identification

Before an application is identified by Application Identification (AppID), the **pre-id-default-policy** options are applied to the session. The session timeout value, along with the required mode of session logging, are applied according to the **pre-id-default-policy** configuration. If there is no configuration within the **pre-id-default-policy** stanza, the default session timeout values are applied to the session and no logs are generated for the **pre-id-default-policy**.

We recommend that customers implement the **set security policies pre-id-default-policy then log session-close** configuration, as shown below, in their own environments.

```
# show security policies pre-id-default-policy
    then {
        log {
            session-close;
            }
        }
```

This configuration will ensure security logs are generated by the SRX if a flow is unable to leave the **pre-id-default-policy**. These events are generally a result of JDPI being unable to properly classify traffic, although they may also indicate potential attempts at evading the APPID engine.

In recent versions of Junos OS, the factory-default configuration of an SRX includes the **session-close** configuration.

CAUTION: Configuring session-init logging for the **pre-id-default-policy** can generate a large amount of logs. Each session that enters the SRX that initially matches the pre-id-default-policy will generate an event. We recommend only using this option for troubleshooting purposes.

SEE ALSO

pre-id-default-policy | 395

Unified Policies Support for Flow

Global Policy Utilization with Unified Policies

Zone-based security policies are prioritized over global policies when a policy lookup is implemented. Starting in Junos OS Release 18.2R1, if a unified policy is configured within the zone-based security policies, then global policy lookup is not performed. Prior to Junos OS Release 18.2R1, if no zone-based policy is matched, then a global policy lookup is performed.

Unified Policy Actions

In a unified policy configuration, specify one of the following actions:

- Permit—Permit the traffic.
- Deny—Drop the traffic and close the session.
- Reject—Notify the client, drop the traffic, and close the session.

SEE ALSO

profile(dynamic-application) | 397

Redirect Profile for Reject Action

Unified policies log drop and reject actions. Unified policies do not notify connected clients for drop and reject actions. The clients are unaware that the webpage is not accessible and might continue their attempts to access it.

Starting in Junos OS Release 18.2R1, a redirect profile can be configured within a unified policy. When a policy blocks HTTP or HTTPS traffic with a deny or reject action, you can define a response in the unified policy to notify the connected clients.

To provide an explanation for the action or to redirect the client to an informative webpage, use the **redirect-message** option at the **[edit security dynamic-application profile *name*]** hierarchy level with the reject or deny action in a unified policy configuration to display a custom message.

When you configure the redirect option, you can specify the custom message or the URL to which the client is redirected.

Limitations to Configuring a Redirect Profile in Unified Policies

There are limitations to configuring a redirect profile in unified policies. They include:

- Support for the redirect action with block messages with a redirect URL are not available for non-HTTP or non-HTTPS applications.
- A unified policy does not check the validity and accessibility of a user-configured redirect URL.
- For clear text processing, out-of-order HTTP packets, or segmented HTTP requests, the available policy actions are reject or deny. A redirect profile is not available.
- The redirect profile can be applied in unified policies only. The reject action for traditional security policies do not support a redirect action with block message profiles or a redirect URL.

SSL Proxy Profile for Reject Action

Starting in Junos OS Release 18.2R1, you can configure a redirect profile within a unified policy. When a policy blocks HTTP or HTTPS traffic with a deny or reject action, you can apply an SSL proxy profile to the traffic. SSL proxy decrypts the traffic and application identification functionality identifies the application. Next, you can take action to redirect or drop the traffic as per the configuration.

Consider the following example:

In this example, you are rejecting some of the Facebook applications such as chat, Farmville, and so on in the policy 'policy-1'. As Facebook is an encrypted application, you need SSL proxy to decrypt the traffic first.

```
policy policy-1 {
    match {
        source-address any;
        destination-address any;
        application any;
        dynamic-application [ junos:FACEBOOK-CHAT junos:FACEBOOK-FARMVILLE
            junos:FACEBOOK-MOBILE-CHAT junos:FACEBOOK-SUPERPOKE
            junos:FACEBOOK-WINDOWSLIVEMESSENGER junos:FACEBOOK-VIDEO ];
    }
    then {
        reject {
            ssl-proxy {
                profile-name test;
            }
        }
        log {
            session-init;
            session-close;
```

```
        }
      }
    }
```

In this example, the policy rejects the encrypted Facebook traffic and applies the configured SSL proxy profile. The SSL proxy decrypts the traffic, and JDPI identifies the application.

Now the policy takes following actions based on your configuration:

- Redirects the client access to other URL, and closes the original session.
- Notifies the client with pre-defined text messages, and closes the session
- Closes the session only. In the example, the policy closes the session.

Match Criteria and Rules for Unified Policies

Unified Policy Implicit and Explicit Match

Starting in Junos OS Release 18.2R1, the command **unified-policy-explicit-match** is introduced at the **[edit security policies]** hierarchy level. This command defines the explicit and implicit policy match behavior and is disabled by default.

- *Explicit match*—If a dependent application does not have any matching policy, then the traffic is dropped if explicit match is enabled. Only those security policies that are explicitly configured for the application are applied.
- *Implicit Match*—If the dependent application does not have any matching policy, then the security policy that is configured for the base application is applied.

By default, the unified policies enforce implicit rules on dependent applications.

In the example shown in Table 23 on page 151, the unified policy P3 is configured for FACEBOOK-ACCESS traffic. HTTP is a dependent application of FACEBOOK-ACCESS and does not have any security policy explicitly configured for it.

Table 23: Example of an Explicit and Implicit Policy Match for a Dependent Application

Dynamic Application	Policy Configured
HTTP	None
FACEBOOK-ACCESS	**P3**

The results for implicit and explicit match behavior is shown in Table 24 on page 152.

Table 24: Example of a Policy Match (Implicit and Explicit Match Criteria)

Application Identified	Policy Matched	Explicit or Implicit Rule Type	Result
None	P3	Implicit (Explicit is not Enabled)	The identified application is HTTP. There is no matching security policy configured for HTTP. The explicit match is not enabled (implicit match), so traffic is further processed until FACEBOOK-ACCESS is identified. The security policy that is configured for FACEBOOK-ACCESS (policy P3) is applied.
HTTP			
FACEBOOK-ACCESS			
HTTP	None	Explicit	The identified application is HTTP. There is no matching policy available for HTTP. The explicit match is enabled, so no security policy is applied in this case.

SEE ALSO

unified-policy-explicit-match | 467

Profile Overlap for Layer 7 Services

While using unified policies, if AppID results have not yet identified the final application, a policy search might return a list of policies instead of a fixed policy. These policies are referred to as potential match policies. Before the final application is identified, a conflict might occur due to multiple policy matches.

In this case, an appropriate profile or default profile is applied for services such as AppQoS, SSL proxy, UTM, and IDP.

SEE ALSO

Understanding Unified Policies [Unified Threat Management (UTM)]

Overview of IDP Policy support for Unified Policies

Policy Rematch

When the **policy rematch** option is enabled, the unified policy allows the device to reevaluate an active session when its associated security policy is modified.

The session remains open if it continues to match the policy that allowed the session initially. The session closes if its associated policy is renamed, deactivated, or deleted. Use the **extensive** option to reevaluate an active session when its associated security policy is renamed, deactivated, or deleted.

If policy rematch is configured in a unified policy before a final match, then rematch behavior might lead to a session closure. After the final match, a policy rematch triggers another policy lookup based on the 6-tuple match criteria and the final identified application.

Configure **policy-rematch** and the **policy-rematch *extensive*** options at the **[edit security policies]** hierarchy level.

SEE ALSO

policy-rematch | **390**

Limitations to Configuring Unified Policies

There are limitations to configuring unified policies. They include:

- An existing session might close in the following cases:
  - When there is a change in the final match for the policy.
  - When a new policy is inserted within the existing policies, and if this new policy is configured with new services.
  - When a final match policy enables new services after the session is created and before the final match.
- Policy-based VPN is not supported for unified policies and can be applied only to the traditional policy.
- ALGs are applied in one of the following conditions:
  - Traditional security policy is configured.
  - Unified policy is configured with dynamic application as none.

  Configuring a dynamic application with **junos:FTP** triggers an FTP ALG to support UTM antivirus scanning. See Enabling FTP Antivirus Scanning (CLI Procedure)
- A security policy that is configured with GPRS might not work if the policy is part of a potential match list.
- A group VPN and user firewall authentication can be applied to a traditional security policy.
- Final policy match information might not be available within session-init logs for policies leveraging dynamic applications.

Example: Configure a Unified Policy Using a Redirect Message Profile

IN THIS SECTION

- Requirements | 154
- Overview | 154
- Configuration | 155
- Verification | 157

This example describes how to configure a unified policy with a redirect message profile. In this example, you configure a redirect profile with a redirect URL. You use the redirect profile as a block message in the policy for traffic in the dynamic applications GMAIL and FACEBOOK-CHAT. Simultaneously, you configure the application **junos-defaults** so that the default port and protocol from the dynamic applications are inherited as the current policy's destination port and protocol match criteria.

Requirements

This example uses the following hardware and software components:

- SRX Series device running Junos OS Release 18.2R1. This configuration example is tested with Junos OS release 18.2R1.

Before you begin, configure security zones. See "Example: Creating Security Zones" on page 29.

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you define the redirect profile as a response when a policy blocks HTTP or HTTPS traffic with a deny or reject action. Through a redirect profile, you provide an explanation for the action or you redirect the client request to an informative webpage when the reject or deny action is applied in a security policy.

To accomplish these objectives, you perform the following tasks:

- Configure the redirect profile with a redirect URL such as http://abc.company.com/information/block-message and use it in the policy as a block message.
- Configure the security policy match criteria **source-address** and **destination-address** with the value **any**.

- Configure the application with **junos-defaults**, so that the default port and protocol from **dynamic-application** is inherited as the current policy's destination port and protocol match criteria.
- Configure **dynamic-application** with **[junos:GMAIL, junos:FACEBOOK-CHAT]** so that the policy can apply the block message profile on the applications.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone trust
set security zones security-zone untrust
set security dynamic-application profile profile1 redirect-message type redirect-url content
    http://abc.company.com/information/block-message
set security policies from-zone trust to-zone untrust policy p2 match source-address any
set security policies from-zone trust to-zone untrust policy p2 match destination-address any
set security policies from-zone trust to-zone untrust policy p2 match application junos-defaults
set security policies from-zone trust to-zone untrust policy p2 match dynamic-application [junos:GMAIL,
    junos:FACEBOOK-CHAT]
set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a unified policy with a redirect message profile:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a profile for the redirect message.

```
[edit security]
user@host# set dynamic-application profile profile1 redirect-message type redirect-url content
    http://abc.company.com/information/block-message
```

3. Create a security policy with a dynamic application as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p2 match source-address any
user@host# set from-zone trust to-zone untrust policy p2 match destination-address any
user@host# set from-zone trust to-zone untrust policy p2 match application junos-defaults
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:GMAIL
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:FACEBOOK-CHAT
```

4. Define the policy action.

```
[edit security policies]
user@host# set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security dynamic-application** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]

user@host# show security policies

```
from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application junos-defaults;
            dynamic-application [ junos:GMAIL, junos:FACEBOOK-CHAT ];
        }
        then {
            reject {
                profile profile1;
            }
        }
```

```
    }
}
```

[edit]

user@host# show security dynamic-application

```
profile profile1 {
    redirect-message {
        type {
            redirect-url {
                content http://abc.company.com/information/block-message;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Unified Policy Configuration | 157

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

From operational mode, enter the **show security policies** command to display a summary of all security policies on the device.

user@host> show security policies

```
Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
 Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
    dynapp-redir-profile: profile1
```

From operational mode, enter the **show security policies detail** command to display a detailed summary of all security policies on the device.

user@host> show security policies detail

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
```

```
    Source port range: [0-0]
    Destination port range: [3128-3128]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8000-8000]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8080-8080]
  IP protocol: 17, ALG: 0, Inactivity timeout: 60
    Source port range: [0-0]
    Destination port range: [1-65535]
Dynamic Application:
  junos:GMAIL: 51
dynapp-redir-profile: profile1
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses
- Configured applications
- Configured dynamic applications
- Policy reject action

SEE ALSO

dynamic-application (Security Policies) | 328

profile(dynamic-application) | 397

Configure a URL Category with Unified Policies

IN THIS SECTION

- Understanding URL Category with Unified Policies | 160
- Example: Configuring a Unified Policy Using URL Category | 160

Understanding URL Category with Unified Policies

Starting from Junos OS Release 18.4R1, the unified policies feature is enhanced to include URL categories as match criteria for web filtering category. URL categories can be configured to unified policies with or without dynamic-application been applied. .

When the URL category is configured as **url-category *any*** to a policy, the policy matches all categories of traffic configured to the unified policies.

When the URL category is configured as **url-category *none*** to a policy, the URL category is not used in the policy look-up. The unified policy configured with **url-category *none*** is considered as the highest priority to policy match for a traffic. When the URL category to a policy is not configured, or when you upgrade a device from previous release to latest release, the URL category of all the policies are considered as **url-category *none***.

Limitations of URL Category with Unified Policies

Using URL categories in an unified policy has the following limitation:

- Only the ports that are generally used such as HTTP and HTTPs traffics are supported by **url-category**. Hence, the policy lookup supports HTTP and HTTPs traffics.

Example: Configuring a Unified Policy Using URL Category

IN THIS SECTION

- Requirements | 161
- Overview | 161
- Configuration | 161
- Verification | 163

This example describes how to configure a unified policy with a URL category.

Requirements

This example uses the following hardware and software components:

- SRX Series device running Junos OS Release 18.4R1. This configuration example is tested with Junos OS release 18.4R1.

Before you begin, configure security zones. See “Example: Creating Security Zones” on page 29.

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, URL category is added to security policy as match criteria for web filtering category.

To accomplish these objectives, you perform the following tasks:

- Configure the security policy match criteria **source-address** and **destination-address** with the value **any**.
- Configure the application with **junos-defaults**, so that the default port and protocol from **dynamic-application** is inherited as the current policy’s destination port and protocol match criteria.
- Configure **dynamic-application** with **[junos:GMAIL, junos:FACEBOOK-CHAT]** so that the policy can apply the block message profile on the applications.
- Configure **url-category** with **Enhanced_News_and_Media** as match criteria for web filtering category.

Configuration

IN THIS SECTION

Step-by-Step Procedure | **162**
Results | **163**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

CLI Quick Configuration

```
set security zones security-zone trust
set security zones security-zone untrust
set security policies from-zone trust to-zone untrust policy p2 match source-address any
set security policies from-zone trust to-zone untrust policy p2 match destination-address any
```

```
set security policies from-zone trust to-zone untrust policy p2 match application junos-defaults
set security policies from-zone trust to-zone untrust policy p2 match dynamic-application [junos:GMAIL,
    junos:FACEBOOK-CHAT]
set security policies from-zone trust to-zone untrust policy p2 match url-category Enhanced_News_and_Media
set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Step-by-Step Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a unified policy with a redirect message profile:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a security policy with a URL category as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p2 match source-address any
user@host# set from-zone trust to-zone untrust policy p2 match destination-address any
user@host# set from-zone trust to-zone untrust policy p2 match application junos-defaults
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:GMAIL
user@host# set security policies from-zone trust to-zone untrust policy p2 match url-category
    Enhanced_News_and_Media
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:FACEBOOK-CHAT
```

3. Define the policy action.

```
[edit security policies]
user@host# set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security dynamic-application** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]

user@host# show security policies

```
from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application junos-defaults;
            dynamic-application [ junos:GMAIL, junos:FACEBOOK-CHAT ];
            url-category Enhanced_News_and_Media;
        }
        then {
            reject {
                profile profile1;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Unified Policy Configuration | **163**

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

From operational mode, enter the **show security policies** command to display a summary of all security policies on the device.

user@host> show security policies

```
Default policy: permit-all
Pre ID default policy: permit-all
From zone: untrust, To zone: internet
  Policy: ip1, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-ping, junos-pingv6, junos-dns-udp, junos-dns-tcp
    Action: permit, log
  Policy: ip2, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: junos-ping, junos-pingv6, junos-telnet, junos-dns-udp,
junos-dns-tcp, junos-ftp, junos-http, junos-https
    Action: permit, log
From zone: untrust, To zone: trust
  Policy: up3, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: H1, H1_v6
    Destination addresses: H0, H0_v6
    Applications: junos-ping, junos-telnet, junos-ftp, junos-http, junos-https,
my_app_udp, my_app_tcp
    Dynamic Applications: junos:HTTP, junos:GOOGLE-GEN, junos:YAHOO, junos:SSL
    Url-category: Enhanced_Search_Engines_and_Portals, cust_white
    Action: permit, log
  Policy: up4, State: enabled, Index: 9, Scope Policy: 0, Sequence number: 2
    Source addresses: as1
    Destination addresses: as0
    Applications: junos-ping, junos-telnet, junos-ftp, junos-http, junos-https,
my_app_udp, my_app_tcp
    Dynamic Applications: junos:web, junos:FTP
    Url-category: Enhanced_Private_IP_Addresses, cust_white
    Action: permit, log
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses
- Configured applications
- Configured dynamic applications
- Configured URL Category
- Policy reject action

Configure Applications in Unified Policies

IN THIS SECTION

- Applications in Unified Policies | **165**
- Example: Configure a Unified Policy Using Dynamic Applications | **166**

Applications in Unified Policies

Starting in Junos OS Release 19.1R1, configuring the **application** statement at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]** hierarchy level is optional if the **dynamic-application** statement is configured at the same hierarchy level.

In releases before Junos OS Release 19.1R1, it is mandatory to configure the **application** statement even if the **dynamic-application** statement is configured.

- When the **application** option is defined then the defined application is used.
- When the **application** option is not defined and the **dynamic-application** option is defined as **any**, then the application **any** is implicitly added.
- When the **application** option is not defined and the **dynamic-application** option is defined (and is not configured as **any**), then the application **junos-defaults** is implicitly added.

Example: Configure a Unified Policy Using Dynamic Applications

IN THIS SECTION

- Requirements | 166
- Overview | 166
- Configuration | 166
- Verification | 168

This example describes how to configure a unified policy using dynamic applications.

Requirements

This example uses the following hardware and software components:

- SRX Series device running Junos OS Release 19.1R1. This configuration example is tested with Junos OS release 19.1R1.

Before you begin, configure security zones. See “Example: Creating Security Zones” on page 29.

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, dynamic applications are added to the security policy as match criteria.

To accomplish these objectives, perform the following tasks:

- Configure the security policy match criteria **source-address** and **destination-address** with the value **any**.
- Configure **dynamic-application** with **[junos:CNN, junos:BBC]** so that the policy can permit the applications junos:CNN and junos:BBC.

Configuration

IN THIS SECTION

- Step-by-Step Procedure | 167
- Results | 168

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

CLI Quick Configuration

```
set security zones security-zone trust
set security zones security-zone untrust
set security policies from-zone trust to-zone untrust policy p3 match source-address any
set security policies from-zone trust to-zone untrust policy p3 match destination-address any
set security policies from-zone trust to-zone untrust policy p3 match dynamic-application junos:CNN
set security policies from-zone trust to-zone untrust policy p3 match dynamic-application junos:BBC
set security policies from-zone trust to-zone untrust policy p3 then permit
```

Step-by-Step Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a unified policy using dynamic applications:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a security policy with a dynamic application as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p3 match source-address any
user@host# set from-zone trust to-zone untrust policy p3 match destination-address any
user@host# set from-zone trust to-zone untrust policy p3 match dynamic-application junos:CNN
user@host# set from-zone trust to-zone untrust policy p3 match dynamic-application junos:BBC
```

3. Define the policy action.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p3 then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]

user@host# show security policies

```
from-zone trust to-zone untrust {
    policy p3 {
        match {
            source-address any;
            destination-address any;
            dynamic-application [ junos:CNN junos:BBC ];
        }
        then {
            permit;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Unified Policy Configuration | **168**

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

From operational mode, enter the **show security policies** command to display a summary of all security policies on the device.

user@host> show security policies

```
Policy: p3, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
  Source addresses: any
  Destination addresses: any
  Applications: junos-defaults
  Dynamic Applications: junos:CNN, junos:BBC
  Action: permit
```

From operational mode, enter the **show security policies detail** command to display a detailed summary of all security policies on the device.

user@host> show security policies detail

```
Default policy: permit-all
Pre ID default policy: permit-all
Policy: p3, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: TCP, ALG: 0, Inactivity timeout: 1800
      Destination ports: 80, 443, 3128, 8000, 8080
  Dynamic Application:
    junos:BBC: 1754
    junos:CNN: 988
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses

- Configured applications

  NOTE: The **Applications** field is autopopulated and its value **junos-defaults** is added implicitly.

- Configured dynamic applications
- Policy action

SEE ALSO

dynamic-application (Security Policies) | 328

Configure Micro-Applications in Unified Policies

IN THIS SECTION

- Limit the Number of Policy Lookups | 170
- Configure Micro-Applications | 171

Starting in Junos OS Release 19.2R1, you can configure micro-applications in a unified policy. Micro-applications are sub-functions of an application. Micro-applications enable granular control of an application at a sub-function level instead of blocking or allowing the entire application. By default, detection of micro-applications is disabled.

The application identification (AppID) module detects an application at a sub-function level on your network. Security policies leverage the application identity information determined by the AppID module. After a specific application is identified, an action such as permit, deny, reject, or redirect is applied to the traffic according to the policy configured on the device. You must enable detection of micro-applications to use them in a security policy. See *Enabling and Disabling Micro-Applications Detection*.

Limit the Number of Policy Lookups

To process a policy, the policy lookup must return the *final match* state for the application. When using a micro-application, application classification does not reach the *final match* state because the

micro-application constantly changes for the session. Because the micro-application changes from one transaction to another, an unlimited number of policy lookups is attempted.

Use the **unified-policy max-lookups** statement at the **[edit security policies]** hierarchy level to limit the number of policy lookups.

SEE ALSO

> *Application Identification Support for Micro-Applications*
>
> max-lookups | **364**

Configure Micro-Applications

To permit a base-level application and all its dependent micro-applications, you can configure a unified policy by specifying the base-level application as a matching criterion. You do not have to explicitly specify each dependent application as matching criteria for the policy. For example, if you specify the base-level application **junos-MODBUS** as a matching criterion in a unified policy, then you don't have to configure the micro-applications of the **junos-MODBUS** application (**junos:MODBUS-READ-COILS** and **junos:MODBUS-WRITE-SINGLE-COIL**) as matching criteria for the policy.

If you want to define a unified policy for granular-level control, then you must specify the micro-applications of the base-level application as matching criteria for the policy. You must not define the base-level application as match criteria in the policy. For more granular-level policy configuration, specify **junos:MODBUS-READ-COILS** as matching criteria in a unified policy. Ensure that the base-level application **junos:MODBUS** is not defined as as a matching criterion in the same unified policy.

Policy Lookup with Micro-Applications

Detection of micro-applications is disabled by default. To use micro-applications as matching criteria for policy lookup, you must enable detection of micro-applications and then specify them as matching criteria for the unified policy. If you have not enabled detection of micro-applications, the application identification (AppID) module does not detect any micro-application and considers the base-level application as the final matching criterion. For example, consider the base-level application **junos-:MODBUS** that has two micro-applications **junos:MODBUS-READ-COILS** and **junos:MODBUS-WRITE-SINGLE-COIL**:

- If you have not enabled detection of micro-applications, **junos:MODBUS** is considered as the *final match* state for the AppID classification. If you enable micro-applications, then you can configure them in a unified policy as any other pre-defined dynamic application. This micro-application is used for policy lookup.
- If you have enabled detection of micro-applications, the AppID module considers **junos:MODBUS** as the *pre-match* state. When the AppID module detects either **junos:MODBUS-READ-COILS** or **junos:MODBUS-WRITE-SINGLE-COIL**, AppID considers this result as the *final match* state and proceeds with policy lookup using this matching criterion.

SEE ALSO

Dynamic Application Classification States

RELATED DOCUMENTATION

Unified Policies Support for Flow

Understanding Unified Policies [Unified Threat Management (UTM)]

Overview of IDP Policy support for Unified Policies

Global Security Policies

IN THIS SECTION

- Global Policy Overview | **172**
- Example: Configuring a Global Policy with No Zone Restrictions | **175**
- Example: Configuring a Global Policy with Multiple Zones | **179**

A security policy is a stateful firewall policy and controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specific IP sources to specific IP destinations at scheduled times. To avoid creating multiple policies across every possible context, you can create a global policy that encompasses all zones, or a multizone policy that encompasses several zones. Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address and also provides access to multiple source zones and multiple destination zones in one policy.

Global Policy Overview

In a Junos OS stateful firewall, security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. Security policies require traffic to enter one security zone and exit another security zone. This combination of a from-zone and to-zone is called a *context*. Each context contains an ordered list of policies. Each policy is processed in the order that it is defined within a context. Traffic is classified by matching the policy's

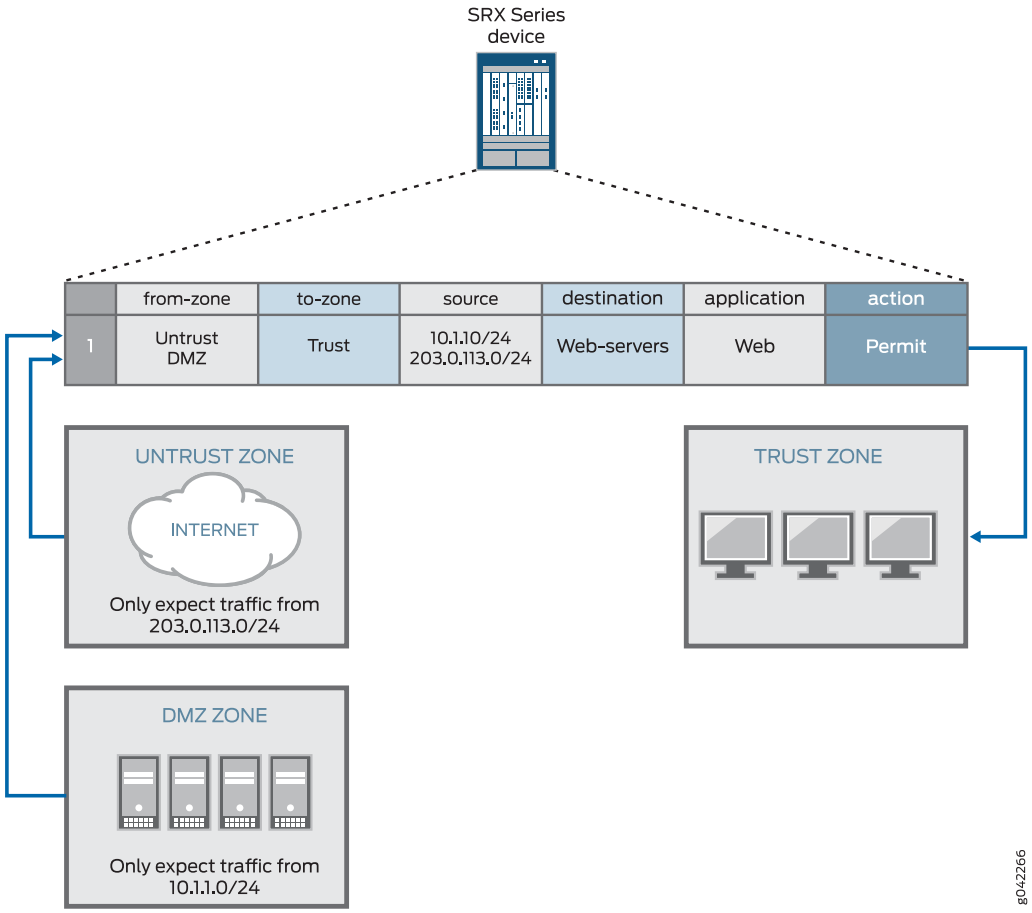
from-zone, to-zone, source address, destination address, and the application that the traffic carries in its protocol header. Each global policy, as with any other security policy, has the following actions: permit, deny, reject, log, count.

You can configure a security policy from the user interface. Security policies control traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specific IP sources to specific IP destinations at scheduled times. This works well in most cases, but it is not flexible enough. For example, if you want to perform actions on traffic you have to configure policies for each possible context. To avoid creating multiple policies across every possible context, you can create a global policy that encompasses all zones, or a multizone policy that encompasses several zones.

Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address “any.” These addresses can span multiple security zones. For example, if you want to provide access to or from multiple zones, you can create a global policy with the address “any,” which encompasses all addresses in all zones. Selecting the “any” address matches any IP address, and when “any” is used as a source/destination address in any global policy configuration, it matches the source/destination address of any packet.

Using a global policy you can also provide access to multiple source zones and multiple destination zones in one policy. However, we recommend that, for security reasons and to avoid spoofing traffic, when you create a multizone policy you use identical matching criteria (source address, destination address, application) and an identical action. In Figure 8 on page 174, for example, if you create a multizone policy that includes DMZ and Untrust from-zones, spoofing traffic from 203.0.113.0/24 from the DMZ zone could match the policy successfully and reach the protected host in the Trust to-zone.

Figure 8: Multizone Global Policy Security Consideration



NOTE: Global policies without from-zone and to-zone information do not support VPN tunnels because VPN tunnels require specific zone information.

When policy lookup is performed, policies are checked in the following order: intra-zone (trust-to-trust), inter-zone (trust-to-untrust), then global. Similar to regular policies, global policies in a context are ordered, such that the first matched policy is applied to the traffic.

NOTE: If you have a global policy, make sure you have not defined a “catch-all” rule such as, match source any, match destination any, or match application any in the intra-zone or inter-zone policies because the global policies will not be checked. If you do not have a global policy, then it is recommended that you include a “deny all” action in your intra-zone or inter-zone policies. If you do have a global policy, then you should include a “deny all” action in the global policy.

In logical systems, you can define global policies for each logical system. Global policies in one logical system are in a separate context than other security policies, and have a lower priority than regular security policies in a policy lookup. For example, if a policy lookup is performed, regular security policies have priority over global policies. Therefore, in a policy lookup, regular security policies are searched first and if there is no match, global policy lookup is performed.

SEE ALSO

Security Policies Overview | 23

Understanding Security Policy Rules | 106

Understanding Security Policy Elements | 105

Example: Configuring a Global Policy with No Zone Restrictions

IN THIS SECTION

- Requirements | 176
- Overview | 176
- Configuration | 176
- Verification | 179

Unlike other security policies in Junos OS, global policies do not reference specific source and destination zones. Global policies reference the predefined address “any” or user-defined addresses that can span multiple security zones. Global policies give you the flexibility of performing actions on traffic without any zone restrictions. For example, you can create a global policy so that every host in every zone can access the company website, for example, www.example.com. Using a global policy is a convenient shortcut when there are many security zones. Traffic is classified by matching its source address, destination address, and the application that the traffic carries in its protocol header.

This example shows how to configure a global policy to deny or permit traffic.

Requirements

Before you begin:

- Review the firewall security policies.

  See “Security Policies Overview” on page 23, “Global Policy Overview” on page 172, “Understanding Security Policy Rules” on page 106, and“Understanding Security Policy Elements” on page 105.

- Configure an address book and create addresses for use in the policy.

  See “Example: Configuring Address Books and Address Sets” on page 53.

- Create an application (or application set) that indicates that the policy applies to traffic of that type.

  See “Example: Configuring Security Policy Applications and Application Sets” on page 71.

Overview

This configuration example shows how to configure a global policy that accomplishes what multiple security policies (using zones) would have accomplished. Global policy gp1 permits all traffic while policy gp2 denies all traffic.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security address-book global address server1 dns-name www.example.com
set security address-book global address server2 dns-name www.mail.example.com
set security policies global policy gp1 match source-address server1
set security policies global policy gp1 match destination-address server2
set security policies global policy gp1 match application any
set security policies global policy gp1 then permit
set security policies global policy gp2 match source-address server2
set security policies global policy gp2 match destination-address server1
set security policies global policy gp2 match application junos-ftp
set security policies global policy gp2 then deny
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

To configure a global policy to permit or deny all traffic:

1. Create addresses.

```
[edit security]
user@host# set security address-book global address server1 dns-name www.example.com
user@host# set security address-book global address server2 dns-name www.mail.example.com
```

2. Create the global policy to permit all traffic.

```
[edit security]
user@host# set policy global policy gp1 match source-address server1
user@host# set policy global policy gp1 match destination-address server2
user@host# set policy global policy gp1 match application any
user@host# set policy global policy gp1 then permit
```

3. Create the global policy to deny all traffic.

```
[edit security]
user@host# set policy global policy gp2 match source-address server2
user@host# set policy global policy gp2 match destination-address server1
user@host# set policy global policy gp2 match application junos-ftp
user@host# set policy global policy gp2 then deny
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show security policies *global*** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

`user@host#` **show security policies**

```
global {
    policy gp1 {
        match {
            source-address server1;
            destination-address server2;
            application any;
        }
```

```
        then {
            permit;
        }
    }
    policy gp2 {
        match {
            source-address server2;
            destination-address server1;
            application junos-ftp;
        }
        then {
            deny;
        }
    }
}
```

`user@host#` **show security policies *global***

```
policy gp1 {
    match {
        source-address server1;
        destination-address server2;
        application any;
    }
    then {
        permit;
    }
}
policy gp2 {
    match {
        source-address server2;
        destination-address server1;
        application junos-ftp;
    }
    then {
        deny;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Global Policy Configuration

Purpose

Verify that global policies gp1 and gp2 are configured as required.

Action

From operational mode, enter the **show security policies *global*** command.

```
user@host> show security policies global
```

```
Global policies:
  Policy: gp1, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: server1
    Destination addresses: server2
    Applications: any
    Action: permit
  Policy: gp2, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 2
    From zones: any
    To zones: any
    Source addresses: server2
    Destination addresses: server1
    Applications: junos-ftp
    Action: deny
```

Meaning

The output displays information about all the global policies configured on the device.

Example: Configuring a Global Policy with Multiple Zones

IN THIS SECTION

- Requirements | **180**
- Overview | **180**

Configuration | 180
Verification | 182

Unlike other security policies in Junos OS, global policies allow you to create multizone policies. A global policy is a convenient shortcut when there are many security zones, because it enables you to configure multiple source zones and multiple destination zones in one global policy instead of having to create a separate policy for each from-zone/to-zone pair, even when other attributes, such as source-address or destination-address, are identical.

Requirements

Before you begin:

- Review the firewall security policies.

  See "Security Policies Overview" on page 23, "Global Policy Overview" on page 172, "Understanding Security Policy Rules" on page 106, and "Understanding Security Policy Elements" on page 105.

- Create security zones.

  See "Example: Creating Security Zones" on page 29

Overview

This configuration example shows how to configure a global policy that accomplishes what multiple security policies would have accomplished. Global policy Pa permits all traffic from zones 1 and 2 to zones 3 and 4.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security policies global policy Pa match source-address any
set security policies global policy Pa match destination-address any
set security policies global policy Pa match application any
set security policies global policy Pa match from-zone zone1
set security policies global policy Pa match from-zone zone2
```

```
set security policies global policy Pa match to-zone zone3
set security policies global policy Pa match to-zone zone4
set security policies global policy Pa then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a global policy with multiple zones:

1. Create a global policy to allow any traffic from zones 1 and 2 to zones 3 and 4.

```
[edit security]
set security policies global policy Pa match source-address any
set security policies global policy Pa match destination-address any
set security policies global policy Pa match application any
set security policies global policy Pa match from-zone zone1
set security policies global policy Pa match from-zone zone2
set security policies global policy Pa match to-zone zone3
set security policies global policy Pa match to-zone zone4
set security policies global policy Pa then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** *global* command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security policies global
policy Pa {
    match {
        source-address any;
        destination-address any;
        application any;
        from-zone [ zone1 zone2 ];
        to-zone [ zone3 zone4 ];
    }
    then {
        permit;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Global Policy Configuration

Purpose

Verify that the global policy is configured as required.

Action

From operational mode, enter the **show security policies** *global* command.

RELATED DOCUMENTATION

Security Policies Overview | 23

Configuring Security Policies | 105

User Role Firewall Security Policies

IN THIS SECTION

- Understanding User Role Firewalls | 183
- User Role Retrieval and the Policy Lookup Process | 183
- Understanding the User Identification Table | 186
- Obtaining Username and Role Information Through Firewall Authentication | 192
- Configuring a User Role Firewall For Captive Portal Redirection | 193
- Example: Configuring a User Role Firewall on an SRX Series Device | 195
- Configuring Resource Policies Using UAC | 203

User role firewall policies allows the administrators to permit or restrict network access for users based on the roles they are assigned. User role firewalls enable greater threat mitigation, provide more informative forensic resources, improve record archiving for regulatory compliance, and enhance routine access provisioning.

Understanding User Role Firewalls

Network security enforcement, monitoring, and reporting based solely on IP information soon will not be sufficient for today's dynamic and mobile workforce. By integrating user firewall policies, administrators can permit or restrict network access of employees, contractors, partners, and other users based on the roles they are assigned. User role firewalls enable greater threat mitigation, provide more informative forensic resources, improve record archiving for regulatory compliance, and enhance routine access provisioning.

User role firewalls trigger two actions:

- Retrieve user and role information associated with the traffic
- Determine the action to take based on six match criteria within the context of the zone pair

The source-identity field distinguishes a user role firewall from other types of firewalls. If the source identity is specified in any policy for a particular zone pair, it is a user role firewall. The user and role information must be retrieved before policy lookup occurs. If the source identity is not specified in any policy, user and role lookup is not required.

To retrieve user and role information, authentication tables are searched for an entry with an IP address corresponding to the traffic. If an entry is found, the user is classified as an authenticated user. If not found, the user is classified as an unauthenticated user.

The username and roles associated with an authenticated user are retrieved for policy matching. Both the authentication classification and the retrieved user and role information are used to match the source-identity field.

Characteristics of the traffic are matched to the policy specifications. Within the zone context, the first policy that matches the user or role and the five standard match criteria determines the action to be applied to the traffic.

The following sections describe the interaction of user and role retrieval and the policy lookup process, methods for acquiring user and role assignments, techniques for configuring user role firewall policies, and an example of configuring user role firewall policies.

User Role Retrieval and the Policy Lookup Process

For policy lookup, firewall policies are grouped by zone pair (the from zone and to zone). Within the context of the zone pair, IP-based firewall policies are matched to traffic based on five criteria—source IP, source port, destination IP, destination port, and protocol.

User role firewall policies include a sixth match criteria—source identity. The source-identity field specifies the users and roles to which the policy applies. When the source-identity field is specified in any policy

within the zone pair, user and role information must be retrieved before policy lookup can proceed. (If all policies in the zone pair are set to **any** or have no entry in the source-identity field, user and role information is not required and the five standard match criteria are used for policy lookup.)

The user identification table (UIT) provides user and role information for an active user who has already been authenticated. Each entry in the table maps an IP address to an authenticated user and any roles associated with that user.

When traffic requires user and role data, each registered UIT is searched for an entry with the same IP address. If a user has not been authenticated, there is no entry for that IP address in the table. If no UIT entry exists, the user is considered an unauthenticated user.

Policy lookup resumes after the user and role information has been retrieved. The characteristics of the traffic are matched against the match criteria in the policies. The source-identity field of a policy can specify one or more users or roles, and the following keywords:

authenticated-user—Users that have been authenticated.

unauthenticated-user—Users that have not been authenticated.

any—All users regardless of authentication. If the source-identity field is not configured or is set to any in all of the policies for the zone pair, only five criteria are matched.

unknown-user—Users unable to be authenticated due to an authentication server disconnection, such as a power outage.

For example, consider user-c who is assigned to the mgmt role. When traffic from the trust zone to the untrust zone is received from user-c at IP address 198.51.100.3, policy lookup is initiated.
Table 25 on page 184 represents three policies in a user role firewall for the trust to untrust zone pair.

Table 25: Trust Zone to Untrust Zone Policy Sequence

src-zone	src-zone	dest-zone	src-IP	dest-IP	source-identity	Application	Action	Services
P1	trust	untrust	192.0.2.0	203.0.113.0	any	http	deny	–
P2	trust	untrust	any	any	mgmt	any	permit	–
P3	trust	untrust	198.51.100.3	any	employee	http	deny	–

All policies for the zone pair are checked first for a source-identity option. If any of the policies specifies a user, a role, or a keyword, user and role retrieval must occur before policy lookup continues.
Table 25 on page 184 shows that policy P2 specifies mgmt as the source identity, making this a user role firewall. User and roles must be retrieved before policy lookup can continue.

> **NOTE:** User and role retrieval would not be performed if the keyword any or if no source identity was specified in all of the policies in the zone context. In such cases, only the five remaining values are matched to the policy criteria.

The UIT represented in Table 26 on page 185 is checked for the IP address. Because the address is found, the username user-c, all roles listed for user-c (in this case, mgmt and employee), and the keyword authenticated-user become data used to match the traffic to the **source-identity** field of a policy.

Table 26: UIT Authentication Details

Source IP Address	Username	Roles
192.0.2.4	user-a	employee
198.51.100.3	user-c	mgmt, employee
203.0.113.2	user-s	contractor

Policy lookup resumes and compares the match criteria in each policy in Table 25 on page 184 to the incoming traffic. Assuming all other criteria match, the first policy that specifies user-c, mgmt, employee, authenticated-user, or any in the source-identity field could be a match for this traffic. Policy P1 matches one of the retrieved roles for user-c, but the source IP address does not match; therefore policy lookup continues. For policy P2, all criteria match the traffic; therefore the policy action is followed and the traffic is permitted. Note that the traffic also matches policy P3, but user firewall policies are terminal—policy lookup ends when the first policy match is found. Because policy P2 matches all criteria, policy lookup ends and policy P3 is not checked.

Policies can also be based on the classification assigned to a user from the user and role retrieval results. Consider a different set of policies for the same zone pair represented by Table 27 on page 185. If traffic is received from user-q at IP 198.51.100.5, user and role retrieval is required because the source-identity field is specified in at least one of the policies.

Table 27: Trust Zone to Untrust Zone Policy Sequence

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	trust	untrust	any	any	un-authenticated-user	http	deny	–
P2	trust	untrust	any	any	mgmt	any	permit	–
P3	trust	untrust	198.51.100.3	any	employee	http	deny	–

When the UIT entries in Table 26 on page 185 are checked, no entry is found for IP address 198.51.100.5. Therefore, the user is considered an unauthenticated user. When policy lookup resumes, the traffic matches policy P1 and the traffic is denied.

Understanding the User Identification Table

IN THIS SECTION

- Local Authentication Table | **187**
- UAC Authentication Table | **189**
- Firewall Authentication Table | **190**
- Policy Provisioning With Users and Roles | **191**

On the SRX Series device, the user identification table (UIT) contains the IP address, username, and role information for each authenticated user. Entries are ordered by IP address. When username and role information is required by a security policy, all UITs are checked. Finding the IP address in an entry in one of the UITs means that the user at that address has already been successfully authenticated.

Each authentication source maintains its own UIT independently and provides query functions for accessing data. Three types of UITs are supported—the local authentication table, the Unified Access Control (UAC) authentication table, and the firewall authentication table.

Local authentication table—A static UIT created on the SRX Series device either manually or programmatically using CLI commands. All users included in the local authentication table are considered authenticated users. When a matching IP address is found, user and role information is retrieved from the table entry and associated with the traffic. User and role information can be created on the device manually or ported from a third-party authentication server, but the data in the local authentication table is not updated in real time.

UAC authentication table—A dynamic UIT pushed from the Junos Pulse Access Control Service to the SRX Series device. The UAC authentication table of a Junos Pulse Access Control Service contains an entry for each authenticated user. The data in this table is updated and pushed to the SRX Series device whenever its authentication table is updated. Depending on the device configuration, authentication could occur on the Junos Pulse Access Control Service itself or on a third-party authentication server. If the Access Control Service is relaying data from a third-party server, the data is restructured by the Access Control Service to match the file format of its authentication table and pushed to the SRX Series device.

Firewall authentication table—A dynamic UIT created on the SRX when **user-firewall** is specified as the firewall authentication type in a security policy. This UIT provides an alternative user role source to UAC when firewall authentication is already in use on your SRX Series device. In this way, users defined for pass-through authentication can also be used as a source for usernames and roles when the **user-firewall** option is specified as the firewall authentication type in a policy.

The **user-firewall** authentication type initiates firewall authentication to verify the user by using either local authentication information or external authentication servers supporting RADIUS, LDAP, or SecureID authentication methods. When this type is specified for firewall authentication, the username and associated groups (roles) from the authentication source are mapped to the IP address and added to the firewall authentication UIT.

Local Authentication Table

The local authentication table is managed with CLI commands that insert or delete entries. A local authentication table can be used as a backup solution when a dynamic UIT is not available, or to assign user and role information to devices that cannot authenticate to the network, such as printers or file servers. The local authentication table can be used for testing or to demonstrate how a user role firewall works without firewall authentication or the Access Control Service configured.

The IP addresses, user names, and roles from a third-party authentication source can be downloaded and added to the local authentication table programmatically using CLI commands. If an authentication source defines users and groups, the groups can be configured as roles and associated with the user as usual.

To be compliant with the UAC authentication table, user names are limited to 65 characters and role names are limited to 64 characters. The local authentication table has a maximum of 10,240 authentication entries on SRX1500 devices and above, 5120 authentication entries on SRX650 devices and below, depending on the Junos OS release in your installation. The local authentication table has 5120 authentication entries on the vSRX. Each authentication entry can be associated with up to 200 roles. The maximum capacity is based on an average of 10 roles assigned to each user. This is the same capacity specified for a UAC authentication table.

Use the following command to add an entry to a local authentication table. Note that each entry is keyed by IP address.

```
user@host> request security user-identification local-authentication-table add user user-name ip-address
    ip-address role [role-name role-name ]
```

The role option in a single CLI command accepts up to 40 roles. To associate more than 40 roles with a single user, you need to enter multiple commands. Keep the following characteristics in mind when adding or modifying authentication user and role entries.

- Role names cannot be the same as usernames.
- Using the **add** option with an existing IP address and username aggregates the role entries. The table can support up to 200 roles per user.
- Using the **add** option with an existing IP address and a new username overwrites the existing username for that IP address.
- Role aggregation does not affect existing sessions.
- To change the role list of an existing entry, you need to delete the existing entry and add an entry with the new role list.
- To change the IP address of an existing entry, you need to delete the existing entry and add an entry with the new IP address.

An entry can be deleted by IP address or by username.

```
user@host> request security user-identification local-authentication-table delete (ip-address | user-name)
```

The local authentication table can be cleared with the following command:

```
user@host> clear security user-identification local-authentication-table
```

To display the content of the local authentication table, use the following **show...** command:

```
user@host> show security user-identification local-authentication-table all (brief | extensive)
```

The **brief** option (the default) displays information in a tabular format sequenced by IP address. User names and role lists are truncated to fit the format.

```
user@host> show security user-identification local-authentication-table all
```

```
Total entries: 2
Source IP       Username            Roles
198.51.100.1       user1            role1
203.0.113.2        user2            role2, role3
```

The **extensive** option displays the full content for each field. Other options limit the display to a single username, IP address, or role.

```
user@host> show security user-identification local-authentication-table all extensive
```

```
Total entries: 3
Ip-address: 198.51.100.2
Username: user1
Roles: role1

Ip-address: 203.0.113.2
Username: user1
Roles: role2

Ip-address: 192.0.2.3
Username: user3
Roles: role1, role2
```

UAC Authentication Table

An SRX Series device can act as an enforcer for a Junos Pulse Access Control Service. In this implementation, the SRX Series device acts as a Layer 3 enforcement point and controls access to resources with IP-based resource policies that have been pushed down from the Access Control Service.

When implemented as a user role firewall, the SRX Series device can access the UAC network in a similar way for user role retrieval. In this instance, user and role information for all authenticated users is pushed from the Access Control Service.

The SRX Series device configuration is similar to that of an enforcer. To establish communication, both devices require configuration and password settings to recognize the other. From the SRX Series device, connect the Access Control Service as an infranet controller.

```
[edit]
user@host# set services unified-access-control infranet-controller ic-name address ip-address
user@host# set services unified-access-control infranet-controller ic-name interface interface-name
user@host# set services unified-access-control infranet-controller ic-name password password
```

From the Access Control Service, define the SRX Series device as a New Enforcer. Use the same password specified on the SRX Series device.

Users and passwords are defined on the Access Control Service as in a standard authentication configuration. One or more roles can also be associated with users. When a user is authenticated, an entry containing the IP address, username, and associated roles is added to the UAC authentication table on the Access Control Service.

The UAC authentication table is pushed from the Access Control Service to the SRX Series device when the connection between the two devices is initialized. Whenever an entry is added, removed, or updated on the Access Control Service, the updated UAC authentication table is pushed to the SRX Series device.

Resource access policies are not necessary on the Access Control Service for a user role firewall implementation. The access behavior is provided in the policy configurations on the SRX Series device. If resource access policies are defined on the Access Control Service, they are pushed to the SRX Series device, but they are not used unless a specific firewall policy implements UAC policies in the policy's action field.

The following **show services** command displays the content of the UAC authentication table on the SRX Series device, confirming that the table has been pushed from the Access Control Service successfully:

```
user@host> show services unified-access-control authentication-table extended
```

```
Id    Source IP       Username     Age   Role name
3     192.0.2.1          april        60    Users
6     192.0.2.2          june         60    Employeees
Total: 2
```

The SRX Series device monitors connections and detects if communication to the Access Control Service has been lost. Based on the UAC configuration, the SRX Series device waits for a response for a configured interval before issuing another request. If a response is received, the Access Control Service is considered functional. If no response is received after a specified timeout period, communication is considered lost and the timeout action is applied. The following UAC command syntax configures the interval, timeout, and timeout action:

```
user@host# set services unified-access-control interval seconds
user@host# set services unified-access-control timeout seconds
user@host# set services unified-access-control timeout-action (close | no-change | open)
```

During a disconnection, if user and role lookup is attempted for the disconnected device, it returns a failure code regardless of the timeout action. If access to all authentication sources is lost, the keyword unknown-user is associated with the IP address. When policy lookup resumes, a policy with unknown-user as the source identity would match the traffic. By implementing a specific policy for unknown-user, you can create a method for handling the loss of authentication sources.

Firewall Authentication Table

Firewall authentication requires users to authenticate to the SRX firewall before permitting access between zones and devices. When traffic is received, the user is prompted for a username and password, and verified

against a specified profile of valid users. Depending on the device configuration, firewall authentication verifies that telnet, HTTP, HTTPS (for SRX5800, SRX5600, and SRX5400 devices), and FTP traffic has been authenticated locally or by a RADIUS, LDAP, or SecureID authentication server.

If firewall authentication is in use on a device, the authentication process can also provide the username and role information needed for user role firewall match criteria. In this case, the information is collected and maintained in a UIT called the firewall authentication table. One or more access policies in the **edit access** hierarchy define authentication methods to be used for firewall authentication.

The firewall authentication table must be enabled as the authentication source for user role information retrieval. The **priority** option specifies the sequence in which all UITs will be checked.

```
user@host# set security user-identification authentication-source firewall-authentication priority priority
```

In a firewall policy for a given zone pair, the **firewall-authentication** service specified for the **permit** action initiates authentication of matching traffic. The **user-firewall** authentication type generates the UIT entry for the authenticated user. The name specified in the **access-profile** option identifies the profile to be used to authenticate valid users.

```
[edit security policies from-zone zone to-zone zone policy policy-name]
user@host# set match source-identity unauthenticated-user
user@host# set then permit firewall-authentication user-firewall access-profile profile-name
```

The UIT table entry contains the IP address of the traffic mapped to the authenticated user and the user's associated groups. When the user is no longer active, the entry is removed from the table. Because entries are continuously added and removed as the traffic and authenticated users change, the firewall authentication table is considered dynamic.

When policies within the same zone pair specify the **source-identity** field as part of its match criteria, all enabled UITs are searched for an entry corresponding to the IP address of the traffic. If found, the associated username and groups are retrieved for source-identity matching. (User authentication group names are considered role names for source-identity matching.)

Policy Provisioning With Users and Roles

All users and roles, whether defined on the SRX Series device or on the Access Control Service, are maintained in a user role file on the SRX Series device. To display all users and roles available for provisioning, use the following **show security...** commands.

> **NOTE:** Usernames and roles in the firewall authentication table are not included in the following displays.

- To display all of the roles that are available for provisioning, use the **show security user-identification role-provision all** command. Note that the roles from all UITs are listed together.
- To display all of the users that are available for provisioning, use the **show security user-identification user-provision all** command.
- To display all of the users and roles that are available for provisioning, use the **show security user-identification source-identity-provision all** command.

When a policy configuration is committed, the user role file is checked to determine if all users and roles specified in the policy are available for provisioning. If a user or role is not found, a warning identifies the missing user or role so that you can define it later.

NOTE: The policy is committed even if a user or role is not yet defined.

SEE ALSO

Acquiring User Role Information from an Active Directory Authentication Server

Obtaining Username and Role Information Through Firewall Authentication

User role firewall policies can be integrated with firewall authentication both to authenticate users and to retrieve username and role information. The information is mapped to the IP address of the traffic, stored in the firewall authentication table, and used for user role firewall policy enforcement.

The following CLI statements configure firewall authentication for user role firewall enforcement.

1. If not already established, define the access profile to be used for firewall authentication. You can skip this step if an existing access profile provides the client data needed for your implementation.

   The access profile is configured in the **[edit access profile]** hierarchy as with other firewall authentication types. It defines clients as firewall users and the passwords that provide them access. Use the following command to define a profile and add client names and passwords for firewall authentication.

   ```
   set access profile profile-name client client-name firewall-user password pwd
   ```

2. If HTTPS traffic is expected, define the access profile to be used for SSL termination services. You can skip this step if an existing SSL termination profile provides the services needed for your implementation.

   The SSL termination profile is configured in the **[edit services ssl]** hierarchy.

```
set services ssl termination profile ssl-profile-name server-certificate certificate-type
```

3. Enable the firewall authentication table as an authentication source.

```
set security user-identification authentication-source firewall-authentication priority priority
```

The priority value determines the sequence in which authentication sources are checked. The default value is 150 for the firewall authentication table. (It is 100 for the local authentication table and 200 for the Unified Access Control (UAC) authentication table.) By default, the local authentication table is checked first, the firewall authentication table is next, and the UAC authentication table is third if it is enabled. You can change this sequence by changing the priority value of one or more of the tables.

4. Configure policies that permit traffic for user firewall authentication.

```
edit security policies from-zone zone to-zone zone policy policy-name
set match source-identity unauthenticated-user
set then permit firewall-authentication user-firewall access-profile profile-name ssl-termination-profile
  profile-name
```

When unauthenticated traffic is permitted for firewall authentication, the user is authenticated based on the access profile configured in this statement. The **ssl-termination-profile** option is needed only for HTTPS traffic.

By specifying the authentication type **user-firewall**, the firewall authentication table is propagated with the IP address, the username, and any group names associated with the authenticated user. (Group names from firewall authentication are interpreted as roles by the user role firewall.) Any further traffic from this IP address will match the IP address in the firewall authentication table, and not require authentication. The associated username and roles are retrieved from the table for use as potential match criteria in subsequent security policies.

Configuring a User Role Firewall For Captive Portal Redirection

To automatically redirect unauthenticated users to the Access Control Service, use the UAC captive portal feature. The following syntax defines the profile for the captive portal:

```
set services unified-access-control captive-portal profile-name redirect-traffic [unauthenticated | all]
set services unified-access-control captive-portal profile-name redirect-url host-url
```

The Kerberos protocol, used for authentication encryption, identifies the Access Control Service only by its service principal name (SPN). The protocol does not accept an IP address. Therefore, the format for the redirect URL must be

```
service://hostname/options
```

In this implementation, the service is HTTP and the hostname is the FQDN of the Access Control Service. Options specified after the hostname pass additional information to the Access Control Service directing the user back to the original destination, to the SRX Series device, or to the policy that originated the redirection. You can configure the options using the following keyword and variable pairs:

?target=%dest-url%—Specifies the protected resource which the user is trying to access.

&enforcer=%enforcer-id%—Specifies the ID assigned to the SRX Series device when it is configured as an enforcer by the Access Control Service.

&policy=%policy-id%—Specifies the encrypted policy ID for the security policy that redirected the traffic.

The following statements define the profile of the captive portal named auth-redirect. The captive-portal redirects unauthenticated users to the URL of the Access Control Service for authentication. After successful authentication, the traffic will be directed back to the SRX Series device.

```
[edit]
user@host# set services unified-access-control captive-portal auth-redirect redirect-traffic unauthenticated
user@host# set services unified-access-control captive-portal auth-redirect redirect-url
   "http://ic6000.example.com/?target=%dest-url%&enforcer=%enforcer-id%&policy=%policy-id%"
```

A defined captive-portal profile is displayed as part of the UAC configuration.

```
[edit]
user@host#show services
```

```
unified-access-control {
    captive-portal auth-redirect {
        redirect-traffic unauthenticated;
        redirect-url
"http://ic6000.example.com/?target=%dest-url%&enforcer=%enforcer-id%&policy=%policy-id%";

    }
}
```

After the profile is defined, a policy can apply the captive portal as an application service when certain criteria is matched. Whenever a user role is unauthenticated, auth-redirect captive portal diverts the traffic from trust zone to untrust zone. The following example defines policy P1 to apply the auth-redirect captive portal profile to any HTTP traffic from the trust to untrust:

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy P1 match application http
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-identity
    unauthenticated-user
user@host# set security policies from-zone trust to-zone untrust policy P1 then permit application-services
    uac-policy captive-portal auth-redirect
```

Example: Configuring a User Role Firewall on an SRX Series Device

IN THIS SECTION

- Requirements | **196**
- Overview | **196**
- Configuration | **197**

The following example configures a user role firewall on an SRX Series device. The firewall controls access from the trust zone to the untrust zone based on active, authenticated users or their associated roles. User role firewall policies establish the following restrictions:

- Only authenticated users are permitted from the trust zone to the untrust zone.

  Unauthenticated users are redirected to an Access Control Service for authentication.

- Traffic from IP 192.0.2.0 to IP 203.0.113.0 within the zone context is restricted. Only the traffic from users with the dev-abc, http-juniper-accessible, or ftp-accessible role is permitted. Permitted traffic is further evaluated by AppFW rules.
  - Permitted traffic identified as junos:FACEBOOK-ACCESS, junos:GOOGLE-TALK, or junos:MEEBO application traffic is denied.
  - Permitted traffic for any other application is permitted.
- All other traffic from the trust zone to the untrust zone is permitted.

Requirements

Before you begin, ensure that the SRX Series device with Junos OS Release 12.1 or later is configured and initialized.

In this example, user and role information associated with the IP address of the traffic is provided by an Access Control Service. For instructions on configuring the Access Control Server, see *Acquiring User Role Information from an Active Directory Authentication Server*.

Overview

Table 28 on page 196 outlines a firewall that meets the requirements for this example. The user role firewall consists of four policies.

Table 28: User Role Firewall Policies

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
user-role-fw1	trust	untrust	any	any	un-authenticated-user	http	permit	UAC captive portal
user-role-fw2	trust	untrust	192.0.2.0	203.0.113.0	dev-abc http-juniper-accessible ftp-accessible	http	permit	AppFW ruleset RS1
user-role-fw3	trust	untrust	192.0.2.0	203.0.113.0	any	http	deny	
user-role-fw4	trust	untrust	any	any	any	http	permit	

Because the **source-identity** field is specified for at least one of the policies in this firewall, user and role information must be retrieved before policy lookup is conducted. The source IP of the traffic is compared to the items in the UIT. If the source IP address is found, the keyword **authenticated**, the username, and any roles associated with this user are stored for later use in policy lookup. If a matching entry for the IP address is not found in the UIT, the keyword **unauthenticated-user** is stored for policy lookup.

After retrieving the username, roles, and keywords, policy lookup begins. Characteristics of the incoming traffic are compared to each policy's match criteria. If a match is found, the action specified in that policy is taken.

A policy match is a terminal event, and no policies after the match are checked. Policy sequence influences the action to be taken for matching traffic. In this example, policies are applied in the following sequence:

user-role-fw1—Applies the UAC captive portal service to matching HTTP traffic with the unauthenticated-user keyword, and redirects it to the Access Control Service for authentication. A UAC profile must also be configured to identify the captive portal specifications.

user-role-fw2—Applies an AppFW rule set to any HTTP traffic from address 192.0.2.0 to address 203.0.113.0 that has a matching username or role. An application firewall must also be configured to define the rule set.

user-role-fw3—Denies all remaining HTTP traffic from address 192.0.2.0 to address 203.0.113.0 for this zone pair.

user-role-fw4—Permits all remaining HTTP traffic for this zone pair.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User guide.

Configuring Redirection For Unauthenticated Users

Step-by-Step Procedure

When an IP address is not listed in the UIT, the unauthenticated-user keyword is used in policy lookup. Instead of denying access to this traffic, a policy can redirect the traffic to a UAC captive portal for authentication.

> **NOTE:** It is important to position a redirection policy for unauthenticated-user before a policy for “any” user so that UAC authentication is not shadowed by a policy intended for authenticated users.

To configure redirection from the SRX Series device to the Access Control Service:

1. From configuration mode, configure the UAC profile for the captive portal acs-device.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device redirect-traffic unauthenticated-user
```

2. Configure the redirection URL for the Access Control Service or a default URL for the captive portal.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device redirect-url
  “https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%”
```

This policy specifies the default target and enforcer variables to be used by the Access Control Service to direct the user back after authentication. This ensures that changes to system specifications will not affect configuration results.

> **NOTE:** When variables, such as **?target=**, are included in the command line, you must enclose the URL and variables in quotation marks.

3. Configure a user role firewall policy that redirects HTTP traffic from zone trust to zone untrust if the source-identity is unauthenticated-user. The captive portal profile name is specified as the action to be taken for traffic matching this policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match source-address
   any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match
   destination-address any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match application
   http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match source-identity
   unauthenticated-user
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 then permit
   application-services uac-policy captive-portal acs-device
```

4. If you are done configuring the policies, commit the changes.

```
[edit]
user@host# commit
```

Results

From configuration mode, confirm your configuration by entering the **show services** and **show security policies** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[edit]

user@host# show services

```
unified-access-control {
 captive-portal acs-device {
```

```
  redirect-traffic unauthenticated;
  redirect-url “https://%ic-ip%/?target=%dest-url%&enforcer=%enforcer-id%”
```

user@host# show security policies

```
from-zone trust to-zone untrust {
 policy user-role-fw1 {
  match {
   source-address any;
   destination-address any;
   application http;
   source-identity unauthenticated-user
  }
  then {
   permit {
    application-services {
     uac-policy {
      captive-portal acs-device;
     }
    }
   }
  }
 }
}
```

Creating a User Role Policy With an Application Firewall

Step-by-Step Procedure

This policy restricts traffic from IP192.0.2.0 to IP 203.0.113.0 based on its user and roles, and also its application. The configuration defines an application rule set and applies it to matching user role traffic.

1. Configure the AppFW rule set rs1. The following rule set denies junos:FACEBOOK-ACCESS, junos:GOOGLE-TALK, or junos:MEEBO application traffic. It applies the default setting, permit, to the remaining traffic.

   [edit security application-firewall rule-sets rs1]
   user@host# **set rule r1 match dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLE-TALK junos:MEEBO]**
   user@host# **set rule r1 then deny**
   user@host# **set default-rule permit**

2. Configure a policy to apply the rs1 application firewall rule set to traffic from IP 192.0.2.0 to IP 203.0.113.0 with the dev-abc, http-mgmt-accessible, or ftp-accessible user role.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match source-address
  192.0.2.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match
  destination-address 203.0.113.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match application
  http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match source-identity
  [dev-abc http-mgmt-accessible ftp-accessible]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 then permit
  application-services application-firewall rule-set rs1
```

3. If you are done configuring the policy, commit the changes.

```
[edit]
user@host# commit
```

Results

Verify that the AppFW rule set is configured properly. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[edit]

user@host# show security application-firewall

```
rule-sets rs1 {
  rule r1 {
   match {
    dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLE-TALK junos:MEEBO]
     }
   then {
    deny;
   }
  }
  default-rule {
   permit;
  }
}
```

Creating Remaining Security Policies Based on User and Role

Step-by-Step Procedure

The following procedure configures policies for the remaining traffic.

1. Configure a policy to deny traffic with the same source and destination address but with different user and role criteria than specified in the user-role-fw2 policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match source-address
   192.0.2.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match
   destination-address 203.0.113.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match application
   http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match source-identity
   any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 then deny
```

2. Configure a security policy to permit all other HTTP traffic from zone trust to zone untrust.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match source-address
   any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match
   destination-address any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match application
   http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match source-identity
   any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 then permit
```

Results

Verify the content and sequence of the user role firewall policies. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[edit]

user@host# show security policies

```
...
from-zone trust to-zone untrust {
 policy user-role-fw1 {
```

```
  match {
   source-address any;
   destination-address any;
   application http;
   source-identity unauthenticated-user
  }
  then {
   permit {
    application-services {
     uac-policy {
      captive-portal acs-device;
     }
    }
   }
  }
 }
}
from-zone trust to-zone untrust {
  policy user-role-fw2 {
   match {
    source-address 192.0.2.0;
    destination-address 203.0.113.0;
    application http;
    source-identity [dev-abc http-juniper-accessible ftp-accessible]
   }
   then {
    permit {
     application-services {
      application-firewall {
       rule-set rs1
      }
     }
    }
   }
  }
}
from-zone trust to-zone untrust {
  policy user-role-fw3 {
   match {
    source-address 192.0.2.0;
    destination-address 203.0.113.0;
    application http;
    source-identity any
   }
```

```
    then {
     deny
    }
   }
}
from-zone trust to-zone untrust {
 policy user-role-fw4 {
  match {
   source-address any;
   destination-address any;
   application http;
   source-identity any
  }
  then {
   permit
  }
 }
}
```

Configuring Resource Policies Using UAC

When using the user role firewall feature, resource policies are not necessary on the Access Control Service. If, however, resource policies exist, they are pushed to the SRX Series device at connection. You can create policies that use these resource policies by applying the UAC application service in the policy configuration. Table 29 on page 203 shows three firewall policies that use the UAC resource policies exclusively:

Table 29: User Role Firewall Usage

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	zone1	zone2	any	192.0.2.1	any	http	permit	UTM
P2	zone1	zone2	any	net2	any	http	permit	IDP
P3	zone1	zone2	any	any	any	any	permit	UAC

The policies for traffic from zone1 to zone2 do not initiate user and role retrieval because any is specified in the source-identity field of every policy. In this example, traffic to the IP address 192.0.2.1 is permitted, but must meet processing requirements for the specified application service, in this case, UTM. Traffic to net2 is permitted and processed by the IDP processing requirements. Any remaining traffic is permitted and processed by the UAC processing requirements.

The configuration for this firewall policy would be as follows:

[edit]

user@host# show security policies

```
from-zone zone1 to-zone zone2 {
 policy P1 {
  match {
   source-address any;
   destination-address 192.0.2.1;
   source-identity any;
   application http;
  }
  then {
    permit {
    application-services {
     idp;
    }
   }
  }
 }
}
from-zone zone1 to-zone zone2 {
 policy P2 {
  match {
   source-address any;
   destination-address net2;
   source-identity any;
   application http;
  }
  then {
    permit {
    application-services {
     utm;
    }
   }
  }
 }
}
from-zone zone1 to-zone zone2 {
 policy P3 {
  match {
   source-address any;
   destination-address any;
```

```
    source-identity any;
    application any;
   }
   then {
     permit {
     application-services {
      uac-policy;
     }
    }
   }
  }
 }
```

In this sample configuration, the action fields in P1 and P2 apply any requirements that have been configured for IDP and UTM respectively. By specifying the uac-policy option, the resource policies pushed to the SRX Series device determine whether the destination is accessible.

A user role firewall can implement both user role policies and the resource policies pushed from the Access Control Service. Table 30 on page 205 shows the policies for three zone pairs.

Table 30: User Role Firewall Usage

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	zone1	zone2	any	any	unauthenticated-user	any	permit	UAC captive portal
P2	zone1	zone2	any	192.0.2.1	role2	http	permit	IDP
P3	zone1	zone2	any	net2	authenticated-user	http	permit	UTM
P4	zone1	zone2	any	any	any	any	permit	
P5	zone1	zone3	any	any	any	any	permit	UAC
P6	zone2	zone3	any	any	any	any	permit	UAC

Traffic from zone1 to zone2 is subject to one of four user role policies. The first of these policies uses the UAC captive portal to redirect unauthenticated users to the Access Control Service for authentication.

The access of traffic from zone1 to zone3 and from zone2 to zone3 is controlled by the resource policies pushed from the Access Control Service.

RELATED DOCUMENTATION

Configuring Security Policies | 105
Monitoring and Troubleshooting Security Policies | 258

Reordering Security Policies

IN THIS SECTION

Understanding Security Policy Ordering | 206
Example: Reordering Security Policies | 208

Reordering security policy allows to move the policies around after they have been created. Junos OS offers a tool for verifying that the order of policies in the policy list is valid.

Understanding Security Policy Ordering

Junos OS offers a tool for verifying that the order of policies in the policy list is valid.

It is possible for one policy to eclipse, or *shadow*, another policy. Consider the following examples:

Example 1

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-services
    all
user@host# set security policies from-zone trust to-zone untrust policy permit-all match source-address any
user@host# set security policies from-zone trust to-zone untrust match destination-address any
user@host# set security policies from-zone trust to-zone untrust match application any
user@host# set security policies from-zone trust to-zone untrust set then permit
user@host# set security policies from-zone untrust to-zone trust policy deny-all match source-address any
user@host# set security policies from-zone untrust to-zone trust policy deny-all match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy deny-all match application any
user@host# set security policies from-zone untrust to-zone trust policy deny-all then deny
```

Example 2

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/2.0 host-inbound-traffic system-services
    all
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services
    all
user@host# set security address-book book1 address mail-untrust 192.0.2.1/24
user@host# set security address-book book1 attach zone untrust
user@host# set security address-book book2 address mail-trust 192.168.1.1/24
user@host# set security address-book book2 attach zone trust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match source-address
    mail-trust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match destination-address
    mail-untrust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match application junos-mail
user@host# set security policies from-zone trust to-zone untrust policy permit-mail then permit
```

In examples 1 and 2, where policy **permit-mail** is configured after policy **permit-all** from zone **trust** to zone **untrust**. All traffic coming from zone **untrust** matches the first policy **permit-all** and is allowed by default. No traffic matches policy **permit-mail**.

Because Junos OS performs a policy lookup starting from the top of the list, when it finds a match for traffic received, it does not look any lower in the policy list. To correct the previous example, you can simply reverse the order of the policies, putting the more specific one first:

```
[edit]
user@host# insert security policies from-zone trust to-zone untrust policy permit-mail before policy permit-all
```

In cases where there are dozens or hundreds of policies, the eclipsing of one policy by another might not be so easy to detect. To check if policies are being shadowed, enter any of the following commands:

```
[edit]
user@host# run show security shadow-policies logical-system lsys-name from-zone from-zone-name to-zone
    to-zone-name
```

```
[edit]
user@host# run show security shadow-policies logical-system lsys-name global
```

This command reports the shadowing and shadowed policies. It is then the administrator's responsibility to correct the situation.

NOTE: The concept of policy *shadowing* refers to the situation where a policy higher in the policy list always takes effect before a subsequent policy. Because the policy lookup always uses the first policy it finds that matches the five-part tuple of the source and destination zone, source and destination address, and application type, if another policy applies to the same tuple (or a subset of the tuple), the policy lookup uses the first policy in the list and never reaches the second one.

SEE ALSO

Security Policies Configuration Overview | 111

Example: Configuring a Security Policy to Permit or Deny All Traffic | 115

Example: Configuring a Security Policy to Permit or Deny Selected Traffic | 120

Example: Reordering Security Policies

IN THIS SECTION

- Requirements | 208
- Overview | 209
- Configuration | 209
- Verification | 209

This example shows show how to move policies around after they have been created.

Requirements

Before you begin:

- Create zones. See "Example: Creating Security Zones" on page 29.
- Configure the address book and create addresses for use in the policy. See "Example: Configuring Address Books and Address Sets" on page 53.

Overview

To reorder policies to correct shadowing, you can simply reverse the order of the policies, putting the more specific one first.

Configuration

Step-by-Step Procedure

To reorder existing policies:

1. Reorder two existing policies by entering the following command:

```
[edit]
user@host# insert security policies from-zone trust to-zone untrust policy permit-mail before policy permit-all
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show security policies** command.

RELATED DOCUMENTATION

Security Policies Overview | 23

Scheduling Security Policies

IN THIS SECTION

- Security Policy Schedulers Overview | 210
- Example: Configuring Schedulers for a Daily Schedule Excluding One Day | 211
- Verifying Scheduled Policies | 214

Scheduler is a security feature that allows a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. You can create schedulers irrespective of a policy, meaning that a scheduler cannot be used by any policies.

Security Policy Schedulers Overview

Schedulers are powerful features that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. You can create schedulers irrespective of a policy, meaning that a scheduler cannot be used by any policies. However, if you want a policy to be active within a scheduled time, then you must first create a scheduler.

When a scheduler times out, the associated policy is deactivated. All sessions associated with the policy are subsequently timed out only if policy-rematch is used

If a policy contains a reference to a scheduler, the schedule determines when the policy is active, that is, when it can be used as a possible match for traffic. Schedulers allow you to restrict access to a resource for a period of time or remove a restriction.

The following guidelines apply to schedulers:

- A scheduler can have multiple policies associated with it; however, a policy cannot be associated with multiple schedulers.
- A policy is active during the time when the scheduler it refers to is also active.
- When a scheduler is off, the policy is unavailable for policy lookup.
- A scheduler can be configured as one of the following:
  - Scheduler can be active for a single time slot, as specified by a start date and time and a stop date and time.
  - Scheduler can be active forever (recurrent), but as specified by the daily schedule. The schedule on a specific day (time slot) takes priority over the daily schedule.
  - Scheduler can be active within a time slot as specified by the weekday schedule.
  - Scheduler can have a combination of two time slots (daily and timeslot).

Example: Configuring Schedulers for a Daily Schedule Excluding One Day

IN THIS SECTION

- Requirements | 211
- Overview | 211
- Configuration | 212
- Verification | 213

This example shows how to configure schedulers for packet match checks every day, from 8:00 AM to 5:00 PM, except Sunday.

Requirements

Before you begin:

- Understand security policies schedulers. See "Security Policies Overview" on page 23.
- Configure security zones before applying this configuration.

Overview

Schedulers are powerful features that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. If you want a policy to be active within a scheduled time, then you must first create a scheduler.

To configure a scheduler, you enter a meaningful name and a start and stop time for the scheduler. You can also attach comments.

In this example, you:

- Specify the scheduler, sch1, that allows a policy, which refers to it, to be used for packet match checks every day, from 8:00 AM to 5:00 PM, except Sunday.

  NOTE: Use the 24-hour format (hh:mm) to specify the hours and minutes for the daily time.

- Create a policy, abc, and specify the match conditions and action to be taken on traffic that matches the specified conditions. and bind the schedulers to the policy to allow access during the specified days.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set schedulers scheduler sch1 daily start-time 08:00 stop-time 17:00
set schedulers scheduler sch1 sunday exclude
set security policies from-zone green to-zone red policy abc match source-address any
set security policies from-zone green to-zone red policy abc match destination-address any
set security policies from-zone green to-zone red policy abc match application any
set security policies from-zone green to-zone red policy abc then permit
set security policies from-zone green to-zone red policy abc scheduler-name sch1
set security policies default-policy permit-all
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a scheduler:

1. Set a scheduler.

   ```
   [edit schedulers ]
   user@host# set scheduler sch1 daily start-time 08:00 stop-time 17:00
   user@host# set scheduler sch1 sunday exclude
   ```

2. Specify the match conditions for the policy.

   ```
   [edit security policies from-zone green to-zone red policy abc]
   user@host# set match source-address any destination-address any application any
   ```

3. Specify the action.

   ```
   [edit security policies from-zone green to-zone red policy abc]
   user@host# set then permit
   ```

4. Associate the scheduler to the policy.

   ```
   [edit security policies from-zone green to-zone red policy abc ]
   ```

```
user@host# set scheduler-name sch1
```

Results

From configuration mode, confirm your configuration by entering the **show schedulers** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
[user@host]show schedulers
   scheduler sch1 {
      daily {
         start-time 08:00 stop-time 17:00;
      sunday exclude;
   }
[edit]
[user@host]show security policies
from-zone green to-zone red {
   policy abc {
      match {
         source-address any;
         destination-address any;
         application any;
      }
      then {
         permit;
      }
      scheduler-name sch1;
   }
}
   default-policy {
      permit-all;
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

IN THIS SECTION

- Verifying Schedulers are Active | **214**
- Verifying Policies | **214**

To confirm that the configuration is working properly, perform these tasks:

Verifying Schedulers are Active

Purpose

Verify if schedulers are enabled or not.

Action

From operational mode, enter the **show schedulers** command.

Verifying Policies

Purpose

Verify if the policies are working.

Action

From operational mode, enter the **show security policies** command.

Verifying Scheduled Policies

Purpose

Display information about scheduled security policies.

Action

Use the **show schedulers** CLI command to display information about schedulers configured on the system. If a specific scheduler is identified, detailed information is displayed for that scheduler only.

`user@host#` **show schedulers**

```
scheduler sche1 {
    /* This is sched1 */
    start-date 2006-11-02.12:12 stop-date 2007-11-02.12:11;
}
scheduler sche2 {
    daily {
        all-day;
    }
    sunday {
        start-time 16:00 stop-time 17:00;
    }
    friday {
        exclude;
    }
```

```
}
scheduler sche3 {
    start-date 2006-11-02.12:12 stop-date 2007-11-02.12:11;
    daily {
        start-time 10:00 stop-time 17:00
    }
    sunday {
        start-time 12:00 stop-time 14:00;
        start-time 16:00 stop-time 17:00;
    }
    monday {
        all-day;
    }
    friday {
        exclude;
    }
}
```

Meaning

The output displays information about schedulers configured on the system. Verify the following information:

- Daily (recurrent) and one-time only (nonrecurrent) schedulers are configured correctly.
- Schedulers are active if policies are associated.

RELATED DOCUMENTATION

Configuring Security Policies | 105

Configuring Security Policies for a VRF Routing Instance

IN THIS SECTION

Overview | 216
Understanding Security Policy Rules | 217

- Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network | **218**
- Example: Configuring a Security Policy to Permit VRF-Based Traffic from an IP Network to an MPLS Network | **224**
- Example: Configuring a Security Policy to Permit VRF-Based Traffic from an MPLS Network to an MPLS Network over GRE without NAT | **229**
- Example: Configuring Security Policies Using VRF Routing Instances in an MPLS Network | **235**

Overview

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service. A policy permits, denies, or tunnels specified types of traffic unidirectionally between two points. Security policies enforce a set of rules for transit traffic, identifying which traffic can pass through the firewall and the actions taken on the traffic as it passes through the firewall. Actions for traffic matching the specified criteria include permit and deny.

When an SRX Series device receives a packet that matches the specifications, it performs the action specified in the policy.

Controlling Traffic in SD-WAN Architecture

In an SD-WAN, the SRX Series device can be configured in a hub and spoke location. You can permit or deny virtual routing and forwarding (VRF) based traffic that enters the device from overlay tunnels by applying firewall policies. You can configure the SRX Series device to permit or deny traffic that is sent to a VRF instance. Configuring the device at the hub location enables you to control all traffic at one location, and provide access to specific network services by applying firewall policies.

Each security policy consists of:

- A unique name for the policy.
- A **from-zone** and a **to-zone**, for example: **user@host# set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone**.
- A set of match criteria defining the conditions that must be satisfied to apply the policy rule. The match criteria are based on a source IP address, destination IP address, and applications. The user identity firewall provides greater granularity by including an additional tuple, such as source-identity, as part of the policy statement.
- A set of actions to be performed in case of a match—permit or deny.

- A set of source VRF names.
- A set of destination VRF names.

> **NOTE:** The configuration options for the source and destination VRF instances are optional. You can configure either the source VRF or a destination VRF, but we recommend that you do not configure both source VRF and destination VRF. The main reason for configuring the source VRF or destination VRF is to differentiate different MPLS labels going through a shared physical network interface.

Table 31 on page 217 lists when to configure the source VRF and destination VRF.

Table 31: Recommendations for Configuring VRF Options

Network Type from Source to Destination	Recommended to Configure Source VRF	Recommended to Configure Destination VRF	VRF Policy Differentiated By
IP network to IP network	No	No	Zones
IP network to MPLS network	No	Yes	Destination VRF
MPLS network to IP network	Yes	No	Source VRF
MPLS network to MPLS network without destination NAT	Yes	No	Source VRF
MPLS network to MPLS network with destination NAT	Yes	Yes	Source VRF and Destination VRF

Understanding Security Policy Rules

A security policy applies security rules to the transit traffic within a context (**from-zone** to **to-zone**). Each policy is uniquely identified by its name. The traffic is classified by matching its source and destination zones, the source and destination addresses, the application, the source VRF, and the destination VRF that the traffic carries in its protocol headers with the policy database in the data plane.

Each policy is associated with the following characteristics:

- A source zone
- A destination zone
- One or many source address names or address set names
- One or many destination address names or address set names
- One or many application names or application set names
- One or many source VRF instances, for example, the VRF routing instance associated with an incoming packet
- One or many destination VRF instances in which the MPLS next hop or destination address route is located

These characteristics are called the match criteria. Each policy also has actions associated with it: permit, deny, and reject. You have to specify the match condition arguments when you configure a policy, source address, destination address, application name, source VRF, and destination VRF.

You can configure either source VRF or destination VRF, but not recommended to configure both source VRF and destination VRF. The main reason for configuring source VRF and destination VR is to differentiate different MPLS labels going through a shared physical network interface. If the source VRF and destination VRF are not configured, then the device determines the source and destination VRF as any.

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network

IN THIS SECTION

- Requirements | **218**
- Overview | **219**
- Configuration | **219**

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF.

Requirements

- Understand how to create a security zone. See “Example: Creating Security Zones” on page 29.

- Supported SRX Series device with Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Configure network interfaces on the device. See *Interfaces User Guide for Security Devices*.

> **NOTE:** An MPLS policy is configurable only when **set security flow advanced-options overlapping-l3vpn** is enabled. By default, this command is disabled.

Overview

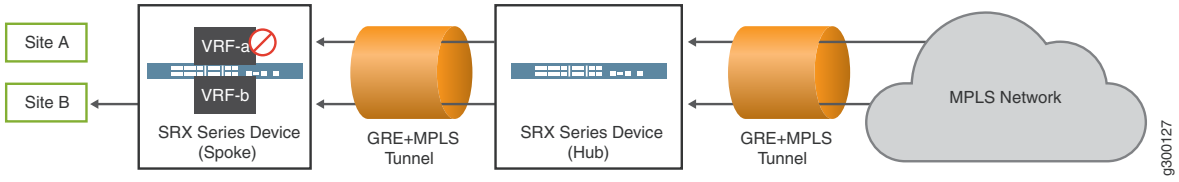
In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 9 on page 219, an SRX Series device is deployed in an SD-WAN to control traffic using the source VRF. Traffic from the MPLS network is sent to site A and site B of the IP network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

This configuration example shows how to:

- Deny traffic to VRF-a (from GRE_Zone-GE_Zone to GRE_Zone)
- Permit traffic to VRF-b (from GRE_Zone-GE_Zone to GRE_Zone)

In this example, the source VRF is configured. We recommend that you configure the source VRF when the destination network points to the MPLS network.

Figure 9: Permitting or Denying VRF-Based Traffic from MPLS Network to an IP Network



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set routing-instances VRF-a instance-type vrf
set routing-instances VRF-a route-distinguisher 10:200
set routing-instances VRF-a vrf-target target:100:100
set routing-instances VRF-a vrf-table-label
set routing-instances VRF-b instance-type vrf
set routing-instances VRF-b route-distinguisher 20:200
set routing-instances VRF-b vrf-target target:200:100
set routing-instances VRF-b vrf-table-label
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-a_policy match source-address
    any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-a_policy match
    destination-address any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-a_policy match application
    any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-a_policy match source-vrf
    VRF-a
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-a_policy then deny
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-b_policy match source-address
    any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-b_policy match
    destination-address any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-b_policy match application
    any
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-b_policy match source-vrf
    VRF-b
set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

   ```
   [edit routing-instances]
   user@host# set VRF-a instance-type vrf
   user@host# set VRF-b instance-type vrf
   ```

2. Assign a route distinguisher to the routing instance.

   ```
   [edit routing-instances]
   user@host# set VRF-a route-distinguisher 10:200
   ```

```
user@host# set VRF-b route-distinguisher 20:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-b vrf-table-label
```

5. Create a security policy to deny VRF-a traffic.

```
[edit security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-vrf VRF-a
user@host# set policy vrf-a_policy then deny
```

6. Create a security policy to permit VRF-b traffic.

```
[edit security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match source-vrf VRF-b
user@host# set policy vrf-b_policy then permit
```

NOTE: If no destination VRF is configured, then the device considers the traffic passes from VRF-a to any-vrf.

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone GRE_Zone-GE_Zone to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-vrf VRF-a;
        }
        then {
            deny;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-vrf VRF-b;
        }
        then {
            permit;
        }
    }
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
```

```
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies** command to display a summary of all the security policies configured on the device.

```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone-GE_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number:
 1
    Source vrf: VRF-a
    destination vrf: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number:
 2
    Source vrf: VRF-b
    destination vrf: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from an IP Network to an MPLS Network

IN THIS SECTION

- Requirements | 224
- Overview | 224
- Configuration | 225

This example shows how to configure a security policy to permit traffic using the destination VRF.

Requirements

- Understand how to create a security zone. See "Example: Creating Security Zones" on page 29.
- Supported SRX Series device with Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Configure network interfaces on the device. See the *Interfaces User Guide for Security Devices*.

> **NOTE:** The MPLS policy is configurable only when **set security flow advanced-options overlapping-l3vpn** is enabled. By default, this command is disabled.

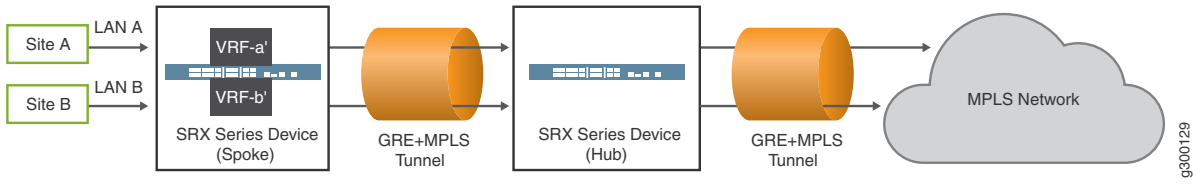
Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device.

In this example, an SRX Series device is deployed in an SD-WAN architecture to control traffic using the destination VRF. You need to configure policies to control the traffic. The default policy does not support VRF options. Traffic from the IP network, that is site A and site B, is sent to the MPLS network. By configuring the policies, you can permit both the traffic from site A and site B to the MPLS network.

In Figure 10 on page 225, the source VRF is not configured as the LAN interface does not belong to an MPLS network. We recommend that you configure the destination VRF when the destination network points to the MPLS network.

Figure 10: Permitting VRF-Based Traffic from an IP Network to an MPLS Network



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set routing-instances VRF-a’ instance-type vrf
set routing-instances VRF-a’ route-distinguisher 10:200
set routing-instances VRF-a’ vrf-target target:100:100
set routing-instances VRF-a’ vrf-table-label
set routing-instances VRF-b’ instance-type vrf
set routing-instances VRF-b’ route-distinguisher 20:200
set routing-instances VRF-b’ vrf-target target:200:100
set routing-instances VRF-b’ vrf-table-label
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match source-address any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match destination-address
    any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match application any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match destination-vrf VRF-a’
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy then permit
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match source-address any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match destination-address
    any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match application any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match destination-vrf VRF-b’
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a policy to permit traffic from the IP network to the MPLS network using the destination VRF:

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host# set VRF-a' instance-type vrf
user@host# set VRF-b' instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a' route-distinguisher 10:200
user@host# set VRF-b' route-distinguisher 20:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a' vrf-target target:100:100
user@host# set VRF-b' vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a' vrf-table-label
user@host# set VRF-b' vrf-table-label
```

5. Create a security policy to permit VRF-a' traffic from the IP network.

```
[edit security policies from-zone LAN-a_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-vrf VRF-a'
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit VRF-b' traffic from the IP network.

```
[edit security policies from-zone LAN-b_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-vrf VRF-b'
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
    from-zone LAN-a_Zone to-zone GRE_Zone {
        policy vrf-a_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                destination-vrf "VRF-a'";
            }
            then {
                permit;
            }
        }
    }
    from-zone LAN-b_Zone to-zone GRE_Zone {
        policy vrf-b_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                destination-vrf "VRF-b'";
            }
            then {
                permit;
            }
        }
    }
```

```
[edit]
user@host# show routing-instances
   VRF-a' {
      instance-type vrf;
      route-distinguisher 10:200;
      vrf-target target:100:100;
      vrf-table-label;
   }
   VRF-b' {
      instance-type vrf;
      route-distinguisher 20:200;
      vrf-target target:200:100;
      vrf-table-label;
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify that the security policy permits VRF-based traffic from the IP network to the MPLS network.

Action

From operational mode, enter the **show security policies** command to display a summary of all the security policies configured on the device.

```
user@host> show security policies
From zone: LAN-a_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number:
 1
    Source vrf: any
    destination vrf: VRF-a'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: LAN-b_Zone, To zone: GRE_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number:
 1
    Source vrf: any
    destination vrf: VRF-b'
    Source addresses: any
    Destination addresses: any
```

```
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from an MPLS Network to an MPLS Network over GRE without NAT

IN THIS SECTION

- Requirements | 229
- Overview | 229
- Configuration | 230

This example shows how to configure a security policy to permit traffic using the source VRF.

Requirements

- Understand how to create a security zone. See "Example: Creating Security Zones" on page 29.
- Supported SRX Series device with Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Configure network interfaces on the device. See the *Interfaces User Guide for Security Devices*.

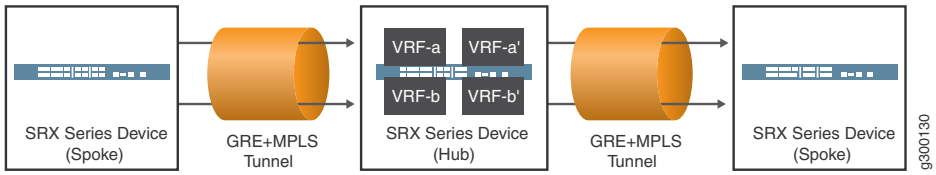
> **NOTE:** The MPLS policy is configurable only when **set security flow advanced-options overlapping-l3vpn** is enabled. By default, this command is disabled.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 11 on page 230, an SRX Series device is deployed in an SD-WAN architecture to control traffic using the source VRF. You need to configure policies to control the traffic. You can permit traffic from an MPLS network to another MPLS network by configuring policies.

We recommend that you configure both the source VRF and the destination VRF when the source and destination are from the MPLS network.

Figure 11: Permitting VRF-Based Traffic from an MPLS Network to an MPLS Network over GRE without NAT



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set routing-instances VRF-a instance-type vrf
set routing-instances VRF-a route-distinguisher 10:200
set routing-instances VRF-a vrf-target target:100:100
set routing-instances VRF-a vrf-table-label
set routing-instances VRF-b instance-type vrf
set routing-instances VRF-b route-distinguisher 20:200
set routing-instances VRF-b vrf-target target:200:100
set routing-instances VRF-b vrf-table-label
set routing-instances VRF-a’ instance-type vrf
set routing-instances VRF-a’ route-distinguisher 30:200
set routing-instances VRF-a’ vrf-target target:300:100
set routing-instances VRF-a’ vrf-table-label
set routing-instances VRF-b’ instance-type vrf
set routing-instances VRF-b’ route-distinguisher 40:200
set routing-instances VRF-b’ vrf-target target:400:100
set routing-instances VRF-b’ vrf-table-label
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match destination-address
    any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-vrf VRF-a
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match destination-vrf
    VRF-a’
```

```
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy then permit
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match destination-address
    any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-vrf VRF-b
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match destination-vrf
    VRF-b'
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a policy to permit traffic from an MPLS network to an MPLS network using source VRF:

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

   ```
   [edit routing-instances]
   user@host# set VRF-a instance-type vrf
   user@host# set VRF-b instance-type vrf
   user@host# set VRF-a' instance-type vrf
   user@host# set VRF-b' instance-type vrf
   ```

2. Assign a route distinguisher to the routing instance.

   ```
   [edit routing-instances]
   user@host# set VRF-a route-distinguisher 10:200
   user@host# set VRF-b route-distinguisher 20:200
   user@host# set VRF-a' route-distinguisher 30:200
   user@host# set VRF-b' route-distinguisher 40:200
   ```

3. Create a community policy to import or export all routes.

   ```
   [edit routing-instances]
   user@host# set VRF-a vrf-target target:100:100
   user@host# set VRF-b vrf-target target:200:100
   user@host# set VRF-a' vrf-target target:300:100
   user@host# set VRF-b' vrf-target target:400:100
   ```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-a' vrf-table-label
user@host# set VRF-b vrf-table-label
user@host# set VRF-b' vrf-table-label
```

5. Create a security policy to permit VRF-a traffic from the MPLS network.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-vrf VRF-a
user@host# set policy vrf-a_policy match destination-vrf VRF-a'
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit VRF-b traffic from the MPLS network.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match source-vrf VRF-b
user@host# set policy vrf-b_policy match destination-vrf VRF-b'
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
   from-zone GRE-1_Zone to-zone GRE-2_Zone {
      policy vrf-a_policy {
         match {
            source-address any;
            destination-address any;
            application any;
```

```
            source-vrf VRF-a;
            destination-vrf "VRF-a'";
        }
        then {
            permit;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-vrf VRF-b;
            destination-vrf "VRF-b'";
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
    VRF-a' {
        instance-type vrf;
        route-distinguisher 30:200;
        vrf-target target:300:100;
        vrf-table-label;
    }
    VRF-b' {
        instance-type vrf;
        route-distinguisher 40:200;
```

```
        vrf-target target:400:100;
        vrf-table-label;
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify that the security policy permits VRF based traffic from the IP network to the MPLS network.

Action

From operational mode, enter the **show security policies** command to display a summary of all the security policies configured on the device.

```
user@host> show security policies
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-a_policy, State: enabled, Index: 7, Scope Policy: 0, Sequence number:
 1
    Source vrf: VRF-a
    destination vrf: VRF-a'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
  Policy: vrf-b_policy, State: enabled, Index: 8, Scope Policy: 0, Sequence number:
 2
    Source vrf: VRF-b
    destination vrf: VRF-b'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring Security Policies Using VRF Routing Instances in an MPLS Network

IN THIS SECTION

- Requirements | 235
- Overview | 235
- MPLS Network to Private IP Network | 236
- Global IP Network to an MPLS Network | 239

This example shows how to configure security policies using VRF routing instances.

Requirements

- Supported SRX Series device with Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Configure network interfaces on the device. See *Interfaces User Guide for Security Devices*.
- Understand how to create a security zone. See "Example: Creating Security Zones" on page 29.

Overview

In this example, you create security policies using virtual routing and forwarding (VRF) instances to isolate traffic traversing in the following networks:

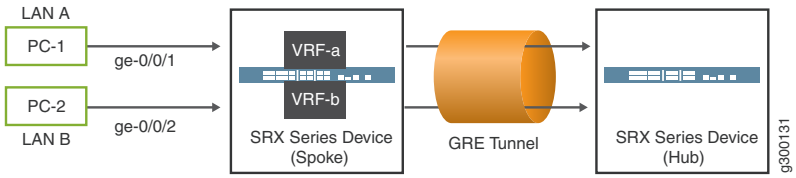
- An MPLS to a private IP network
- A Global IP to an MPLS network

MPLS Network to Private IP Network

Different sites that connect to a spoke-side SRX Series device can belong to the same tenant or to the same VRF routing instance. These sites send IP traffic that is intended to reach either public Internet or remote tenant sites (LAN A and LAN B). In this example, traffic from VRF instances VRF-a and VRF-b enters the SRX Series device from same overlay tunnel (GRE tunnel). When the traffic reaches the spoke-side SRX Series device, you must create security policies on the SRX Series device using VRFs as the match criteria. The traffic matching the VRF is permitted to the destination.

Figure 12 on page 236 shows the topology used in this example.

Figure 12: MPLS to Private IP Network Topology



In this example, you create the following policies:

- Policy vrf-a-policy to permit traffic from the VRF-a routing instance to the device in LAN A.
- Policy vrf-b-policy to permit traffic from the VRF-b routing instance to the device in LAN B.

Step-by-Step Procedure

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host#set VRF-a instance-type vrf
user@host#set VRF-b instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a route-distinguisher 10:200
user@host# set VRF-b route-distinguisher 20:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
```

```
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-b vrf-table-label
```

5. Create a security policy to permit traffic from VRF-a destined for LAN A.

```
[edit security policies from-zone GRE_Zone to-zone LAN-a_Zone]
set policy vrf-a_policy match source-address any
set policy vrf-a_policy match destination-address any
set policy vrf-a_policy match application any
set policy vrf-a_policy match source-vrf VRF-a
set policy vrf-a_policy then permit
```

6. Create a security policy to permit traffic from VRF-b destined for LAN B.

```
[edit security policies from-zone GRE_Zone to-zone LAN-b_Zone]
set policy vrf-b_policy match source-address any
set policy vrf-b_policy match destination-address any
set policy vrf-b_policy match application any
set policy vrf-b_policy match source-vrf VRF-b
set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show security policies
from-zone GRE_Zone to-zone LAN-a_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
```

```
        }
        then {
            permit;
        }
    }
}
from-zone GRE_Zone to-zone LAN-b_Zone {
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-vrf VRF-b;
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

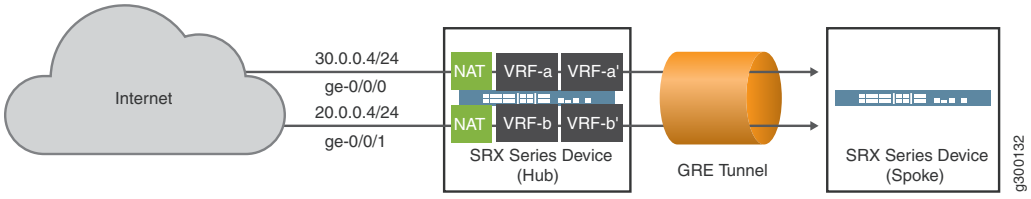
Global IP Network to an MPLS Network

This example shows an SD-WAN deployment where traffic from the public Internet attempts to reach per VRF private network servers.

In this example, you configure the SRX Series device with a destination NAT to convert a public IP address to per private IP addresses.

Figure 13 on page 240 shows the topology used in this example.

Figure 13: Global IP Network to MPLS Network Topology



In the topology, devices in the untrust zone (GE_Zone) access a server in the trust zone (GRE_Zone) by way of public IP address. For packets that enter the SRX Series device from the untrust zone with the destination IP address 50.0.0.4/24, the destination IP address is translated to the private address 30.0.0.4/24. Similarly, for traffic entering the SRX Series device with the destination IP address 40.0.0.4/24, the destination IP address is translated to the private address 20.0.0.4/24.

An IP address pool is configured per VRF instance (VRF-a and VRF-b).

The NAT rule search uses the VRF routing instances (VRF-a and VRF-b) that are configured as matching criteria. NAT rule results with the VRF routing instance and NAT information are used in the destination route look-up.

NOTE: An MPLS policy is configurable only when **set security flow advanced-options overlapping-l3vpn** is enabled.

NOTE: Virtual router or vrf router with **set security flow advanced-options overlapping-l3vpn** enabled must be defined under [**routing-instances**] hierarchy level.

This example describes the following configurations:

- Destination NAT pool vrf-a_p that contains the IP address 30.0.0.4/24 and associated with the VRF VRF-a.
- Destination NAT pool vrf-b_p that contains the IP address 20.0.0.4/24 and associated with the VRF VRF-b.

- Destination NAT rule set rs with rule vrf-a_r to match packets received from the ge-0/0/0.0 interface with the destination IP address 40.0.0.0/24.
- Destination NAT rule set rs with rule vrf-b_r to match packets received from the ge-0/0/1.0 interface with the destination IP address 50.0.0.0/24.
- For matching packets, the destination address is translated to the address in vrf-a_p and vrf-a_b respectively.
- Security policies to permit traffic from the untrust zone (GE_Zone) to the translated destination IP address in the trust zone (GRE_Zone).

Step-by-Step Procedure

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host# set VRF-a instance-type vrf
user@host# set VRF-b instance-type vrf
user@host# set VRF-a' instance-type vrf
user@host# set VRF-b' instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a route-distinguisher 10:200
user@host# set VRF-b route-distinguisher 20:200
user@host# set VRF-a' route-distinguisher 30:200
user@host# set VRF-b' route-distinguisher 40:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
user@host# set VRF-a' vrf-target target:300:100
user@host# set VRF-b' vrf-target target:400:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
```

```
user@host# set VRF-a' vrf-table-label
user@host# set VRF-b vrf-table-label
user@host# set VRF-b' vrf-table-label
```

5. Create the destination NAT pool.

```
[edit security nat destination]
user@host# set pool vrf-a_p routing-instance VRF-a
user@host# set pool vrf-a_p address 20.0.0.4/24
user@host# set pool vrf-b_p routing-instance VRF-b
user@host# set pool vrf-b_p address 30.0.0.4/24
```

6. Create a destination NAT rule set.

```
[edit security nat destination]
user@host# set rule-set rs from interface ge-0/0/0.0
user@host# set rule-set rs rule vrf-a_r match destination-address 40.0.0.4/24
user@host# set rule-set rs rule vrf-a_r then destination-nat pool vrf-a_p
```

7. Configure a rule that matches packets and translates the destination address to the address in the pool.

```
[edit security nat destination]
user@host# set rule-set rs from interface ge-0/0/1.0
user@host# set rule-set rs rule vrf-b_r match destination-address 50.0.0.4/24
user@host# set rule-set rs rule vrf-b_r then destination-nat pool vrf-b_p
```

8. Configure a security policy that allows traffic from the untrust zone to the server in the trust zone.

```
[edit security policies from-zone internet to-zone trust]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy_policy match application any
user@host# set policy vrf-a_policy match destination-vrf VRF-a'
user@host# set policy vrf-a_policy then permit
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-vrf VRF-b'
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies**, **show routing-instances**, and the **show security nat** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show security policies
from-zone internet to-zone trust {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-vrf VRF-a;
        }
        then {
            permit;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-vrf VRF-b;
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
```

```
        vrf-table-label;
    }
    VRF-a' {
        instance-type vrf;
        route-distinguisher 30:200;
        vrf-target target:300:100;
        vrf-table-label;
    }
    VRF-b' {
        instance-type vrf;
        route-distinguisher 40:200;
        vrf-target target:400:100;
        vrf-table-label;
    }
```

```
user@host# show security nat destination
pool vrf-a_p {
    routing-instance {
        VRF-a';
    }
    address 20.0.0.4/24;
}
pool vrf-b_p {
    routing-instance {
        VRF-b';
    }
    address 30.0.0.4/24;
}
rule-set rs {
    from interface [ ge-0/0/0.0 ge-0/0/1.0 ];
    rule vrf-a_r {
        match {
            destination-address 40.0.0.4/24;
        }
        then {
            destination-nat {
                pool {
                    vrf-a_p;
                }
            }
        }
    }
    rule vrf-b_r {
        match {
```

```
        destination-address 50.0.0.4/24;
      }
      then {
        destination-nat {
          pool {
            vrf-b_p;
          }
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the Destination NAT Rule

Purpose

Display information about all the destination NAT rules.

Action

From operational mode, enter the **show security nat destination rule all** command.

```
user@host> show security nat destination rule all
Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 6/0
Destination NAT rule: rule1                  Rule-set: vrf-b_r
  Rule-Id                   : 2
  Rule position             : 2
  From routing instance     : vrf-b_r
  Destination addresses     : 50.0.0.4         - 50.0.0.4
  Action                    : vrf-b_p
  Translation hits          : 0
    Successful sessions     : 0
    Failed sessions         : 0
  Number of sessions        : 0
```

[...Output truncated...]

Meaning

The command displays the destination NAT rule. View the Translation hits field to check for traffic that matches the destination rule.

Verifying Flow Session

Purpose

Display information about all the currently active security sessions on the device.

Action

From operational mode, enter the **show security flow session** command.

```
user@host>show security flow session
Flow Sessions on FPC0 PIC1:
Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
In: 203.0.113.11/1000  203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.1, VRF:
VRF-a, Pkts: 1, Bytes: 86, CP Session ID: 10320276
Out: 203.0.113.1/2000  203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0, VRF:
VRF-b, Pkts: 0, Bytes: 0, CP Session ID: 10320276
```

Meaning

The command displays details about all the active sessions. View the VRF field to check the VRF routing instance details in the flow.

RELATED DOCUMENTATION

- *Flow Management in SRX Series Devices Using VRF Routing Instance*
- *Understanding ALG Support for VRF Routing Instance*
- *NAT for VRF Routing Instance*

Configuring Security Policies Using VRF Group

IN THIS SECTION

- Overview | **247**
- Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network using Source VRF Group | **248**

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from an IP Network to MPLS Network using Destination VRF Group | 252

Managing Overlapping VPN using VRF group | 257

Overview

In SD-WAN network, when different VRF based traffic enter the device from same tunnel such as GRE or GE, the device applies policy based on the given VRF instance. The device either permit or deny traffic destined to a particular VRF instance to control the VRF based traffic.

Currently, there are 5 matching conditions for each policy:

- From zone
- To zone
- Source address
- Destination address
- Applications

Figure 14 on page 247 shows the match conditions in a policy.

Figure 14: Match Conditions

	Match Conditions					Action
	From-Zone	To-Zone	SRC-Add	DST-Add	App	
P1	Z1	Z2	any	any	https	permit/UTM

g300280

With the current policy matching conditions, you cannot permit VRF-B1 or VRF-B2 and deny VRF-A1 or VRF-A2. To support this, additional matching conditions are added to the policy in the SD-WAN network using VRF group.

When the flow receives the information of source and destination VRF groups, it forwards the information to policy search API along with the policy key tuple information to meet the match conditions.

Figure 15 on page 248 shows the VRF groups added as match condition in a policy.

Figure 15: Match Conditions with VRF group

	Match Conditions							Action
	From-Zone	To-Zone	SRC-Add	DST-Add	App	source-l3vpn-vrf-group	Destination-l3vpn-vrf-group	
vpn-a_policy	GRE_Zone	GRE_Zone/GE_Zone	any	any	any	VRF-GRP_A	VRF-GRP_A'	deny
vpn-b_policy	GRE_Zone	GRE_Zone/GE_Zone	any	any	any	VRF-GRP_B	VRF-GRP_B'	permit

g300279

NOTE: If the source and destination VRF group information is not specified in a policy, then these groups matches **any** VRF group.

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from MPLS Network to an IP Network using Source VRF Group

IN THIS SECTION

- Requirements | 248
- Overview | 249
- Configuration | 249

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF group.

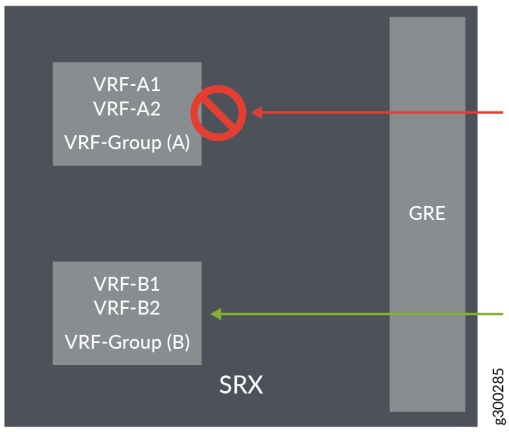
Requirements

- Understand how to create a security zone. See “Example: Creating Security Zones” on page 29.
- Supported SRX Series device with Junos OS Release 15.1X49-D170 or later. This configuration example is tested for Junos OS Release 15.1X49-D170.
- Configure network interfaces on the device. See *Interfaces User Guide for Security Devices*.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 16 on page 249, an SRX Series device is deployed in an SD-WAN to control traffic using the source VRF group. Traffic from the GRE MPLS network is sent to site A and site B of the IP network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

Figure 16: Policy Control from MPLS network



This configuration example shows how to:

- Deny traffic from vpn-A (from GRE MPLS)
- Permit traffic from vpn-B (from GRE MPLS)

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-a_policy match source-address any
```

```
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-a_policy match destination-address
    any
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-a_policy match application any
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-a_policy match source-l3vpn-vrf-group
    vpn-A
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-a_policy then deny
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-b_policy match source-address any
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-b_policy match destination-address
    any
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-b_policy match application any
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-b_policy match source-l3vpn-vrf-group
    vpn-B
set security policies from-zone GRE_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Create VRF group vpn-A with VRF instances A1 and A2

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-B with VRF instances B1 and B2

```
[edit security]
user@host# set l3vpn vrf-group vpn-B vrf VRF-B1
user@host# set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Create a security policy to deny vpn-A traffic.

```
[edit security policies from-zone GRE_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then deny
```

4. Create a security policy to permit vpn-B traffic.

```
[edit security policies from-zone GRE_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match source-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone GRE_Zone to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group vpn-A;
        }
        then {
            deny;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group vpn-B;
        }
        then {
            permit;
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies** command to display a summary of all the security policies configured on the device.

```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone-GE_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number:
 1
    Source L3VPN VRF Group: vpn-A
    destination L3VPN vrf-group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number:
 2
    Source L3VPN VRF Group: vpn-B
    destination L3VPN vrf-group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit or Deny VRF-Based Traffic from an IP Network to MPLS Network using Destination VRF Group

IN THIS SECTION

- Requirements | **253**
- Overview | **253**
- Configuration | **253**

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF group.

Requirements

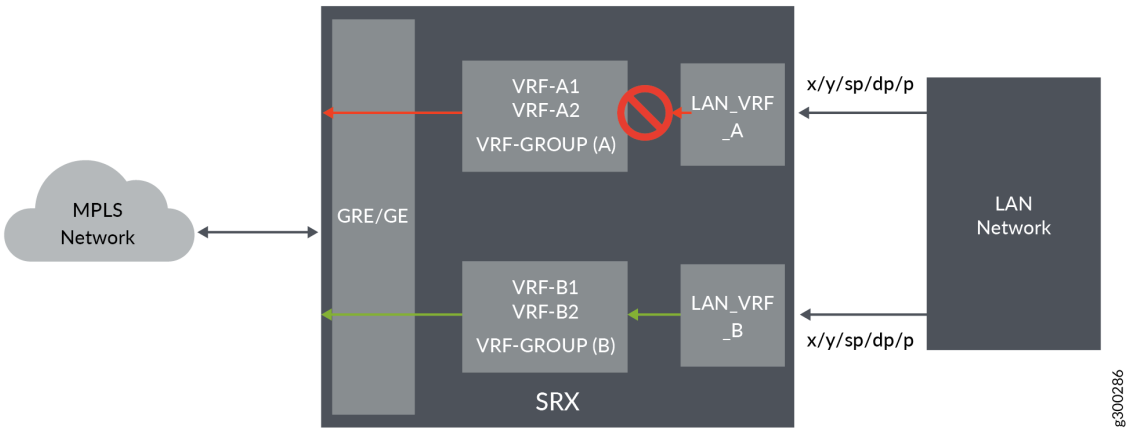
- Understand how to create a security zone. See "Example: Creating Security Zones" on page 29.
- Supported SRX Series device with Junos OS Release 15.1X49-D170 or later. This configuration example is tested for Junos OS Release 15.1X49-D170.
- Configure network interfaces on the device. See *Interfaces User Guide for Security Devices*.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 17 on page 253, an SRX Series device is deployed in an SD-WAN to control traffic using the destination VRF group. Traffic from IP network is sent to site A and site B of the GRE MPLS network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

This configuration example shows how to:

Figure 17: Policy control to MPLS network



- Deny traffic to vpn-A (to GRE MPLS)
- Permit traffic to vpn-B (to GRE MPLS)

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match source-address any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match destination-address
   any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match application any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match
   destination-l3vpn-vrf-group vpn-A
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy then deny
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match source-address any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match destination-address
   any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match application any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match
   destination-l3vpn-vrf-group vpn-B
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Create VRF group vpn-A with VRF instances A1 and A2

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-B with VRF instances B1 and B2

```
[edit security]
user@host# set l3vpn vrf-group vpn-B vrf VRF-B1
user@host# set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Create a security policy to deny vpn-A traffic.

```
[edit security policies from-zone LAN-a_Zone to-zone GRE_Zone]
```

```
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then deny
```

4. Create a security policy to permit vpn-B traffic.

```
[edit security policies from-zone LAN-b_Zone e to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the **show security policies** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
from-zone LAN-a_Zone to-zone GRE_Zone {
   policy vrf-a_policy {
      match {
         source-address any;
         destination-address any;
         application any;
         destination-l3vpn-vrf-group vpn-A;
      }
      then {
         deny;
      }
   }
}
   from-zone LAN-b_Zone to-zone GRE_Zone {
   policy vrf-b_policy {
      match {
         source-address any;
         destination-address any;
         application any;
         destination-l3vpn-vrf-group vpn-B;
```

```
      }
      then {
         permit;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

From operational mode, enter the **show security policies** command to display a summary of all the security policies configured on the device.

```
user@root> show security policies
Default policy: permit-all
From zone:  LAN-a_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number:
 1
    Source L3VPN VRF Group: any
    destination L3VPN vrf-group: vpn-A
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny
 From zone:  LAN-b_Zone, To zone: GRE_Zone
 Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number:
 2
    Source L3VPN VRF Group: any
    destination L3VPN vrf-group: vpn-B
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Managing Overlapping VPN using VRF group

When there are two sessions in a L3VPN network, to avoid any conflicts between the two sessions VRF group-ID is added to session key as an additional key to differentiate the sessions.

In Figure 18 on page 257 network1 and network3 are grouped together to VRF group-A in L3VPN network, and network2 and network4 are grouped together to VRF group-B. The sessions use VRF group-A and VRF group-B as differentiators.

Figure 18: Overlapping VPN using VRF groups

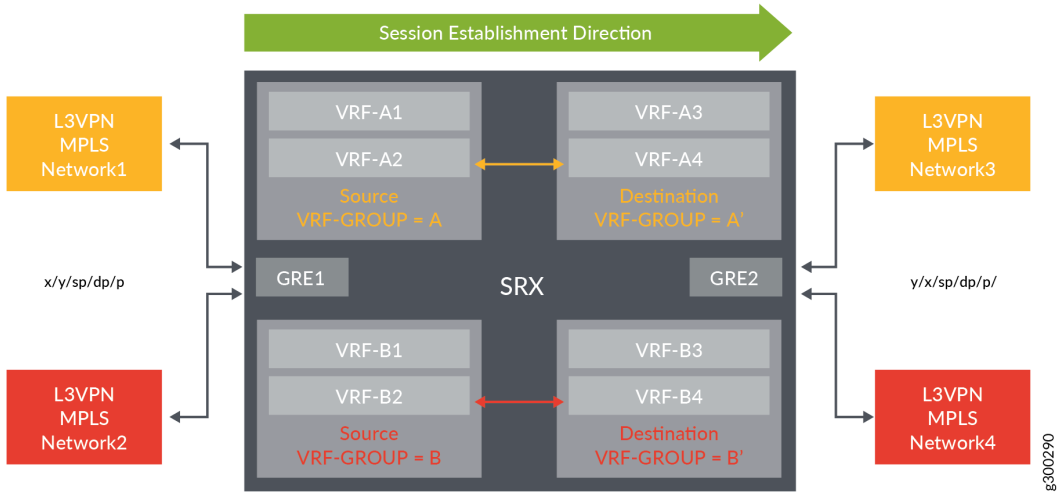


Table 32 on page 257

Table 32: L3VPN Session Information

L3VPN Network 1 and 3 session		L3VPN Network 2 and 4 session	
(Forward)	(Reverse)	(Forward)	(Reverse)
5-tuple: x/y/sp/dp/p	5-tuple: y/x/dp/sp/p	5-tuple: x/y/sp/dp/p	5-tuple: y/x/dp/sp/p
Token: GRE1(zone_id+VR_id) + VRF group-ID (A)	Token: GRE1(zone_id+VR_id) + VRF group-ID (B)	Token: GRE1(zone_id+VR_id) + VRF group-ID (A')	Token: GRE1(zone_id+VR_id) + VRF group-ID (B')

RELATED DOCUMENTATION

Monitoring and Troubleshooting Security Policies

IN THIS SECTION

- Understanding Security Alarms | **258**
- Example: Generating a Security Alarm in Response to Policy Violations | **259**
- Matching Security Policies | **262**
- Tracking Policy Hit Counts | **264**
- Checking Memory Usage on SRX Series Devices | **264**
- Monitoring Security Policy Statistics | **266**
- Verifying Shadow Policies | **266**
- Troubleshooting Security Policies | **269**
- High Availability (HA) Synchronization of Address Name Resolving Cache | **271**

Monitoring provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and effect operational conditions. Troubleshooting provides contextual guidance for resolving the access issues on networks. You can then address user concerns and provide resolution in a timely manner.

Understanding Security Alarms

Alarms are triggered when packets are dropped because of a policy violation. A policy violation occurs when a packet matches a reject or deny policy. A policy violation alarm is generated when the system monitors any of the following audited events:

- Number of policy violations by a source network identifier within a specified period
- Number of policy violations to a destination network identifier within a specified period
- Number of policy violations to an application within a specified period
- Policy rule or group of rule violations within a specified period

There are four types of alarms corresponding to these four events. The alarms are based on source IP, destination IP, application, and policy.

When a packet encounters a reject or deny policy, the policy violation counters for all enabled types of alarm are increased. When any counter reaches the specified threshold within a specified period, an alarm is generated. After a specified period, the policy violation counter is reset and reused to start another counting cycle.

To view the alarm information, run the **show security alarms** command. The violation count and the alarm do not persist across system reboots. After a reboot, the violation count resets to zero and the alarm is cleared from the alarm queue.

After taking appropriate actions, you can clear the alarm. The alarm remains in the queue until you clear it (or until you reboot the device). To clear the alarm, run the **clear security alarms** command. After you clear the alarm, a subsequent series of flow policy violations can cause a new alarm to be raised.

SEE ALSO

Example: Setting an Audible Alert as Notification of a Security Alarm

Example: Generating a Security Alarm in Response to Policy Violations

IN THIS SECTION

- Requirements | **259**
- Overview | **260**
- Configuration | **260**
- Verification | **262**

This example shows how to configure the device to generate a system alarm when a policy violation occurs. By default, no alarm is raised when a policy violation occurs.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you configure an alarm to be raised when:

- The application size is 10240 units.
- The source IP violation exceeds 1000 within 20 seconds.
- The destination IP violations exceeds 1000 within 10 seconds.
- The policy match violation exceeds 100, with a size of 100 units.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level , and then enter **commit** from configuration mode.

```
set security alarms potential-violation policy application size 10240
set security alarms potential-violation policy source-ip threshold 1000 duration 20
set security alarms potential-violation policy destination-ip threshold 1000 duration 10
set security alarms potential-violation policy policy-match threshold 100 size 100
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure policy violation alarms:

1. Enable security alarms.

   ```
   [edit]
   user@host# edit security alarms
   ```

2. Specify that an alarm should be raised when an application violation occurs.

   ```
   [edit security alarms potential-violation policy]
   user@host# set application size 10240
   ```

3. Specify that an alarm should be raised when a source IP violation occurs.

   ```
   [edit security alarms potential-violation policy]
   ```

```
user@host# set source-ip threshold 1000 duration 20
```

4. Specify that an alarm should be raised when a destination IP violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set destination-ip threshold 1000 duration 10
```

5. Specify that an alarm should be raised when a policy match violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set policy-match threshold 100 size 100
```

Results

From configuration mode, confirm your configuration by entering the **show security alarms** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
policy {
    source-ip {
        threshold 1000;
        duration 20;
    }
    destination-ip {
        threshold 1000;
        duration 10;
    }
    application {
        size 10240;
    }
    policy-match {
        threshold 100;
        size 100;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, from operational mode, enter the **show security alarms** command.

Matching Security Policies

The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are “shadowed” by the first and are never encountered by matching traffic.

> **NOTE:** The **show security match-policies** command is applicable only to security policies; IDP policies are not supported.

Example 1: show security match-policies

`user@host>` **show security match-policies from-zone z1 to-zone z2 source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp**

```
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 203.0.113.1/25
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 203.0.113.129/25
    d3: 192.0.2.1/24
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [21-21]
```

Example 2: Using the result-count Option

By default, the output list contains the policy that will be applied to traffic with the specified characteristics. To list more than one policy that match the criteria, use the **result-count** option. The first policy listed is always the policy that will be applied to matching traffic. If the **result-count** value is from 2 to 16, the output includes all policies that match the criteria up to the specified **result-count**. All policies listed after the first are "shadowed" by the first policy and are never applied to matching traffic.

Use this option to test the positioning of a new policy or to troubleshoot a policy that is not applied as expected for particular traffic.

In the following example, the traffic criteria matches two policies. The first policy listed, **p1**, contains the action applied to the traffic. Policy **p15** is shadowed by the first policy, and its action, therefore, will not be applied to matching traffic.

`user@host>` **show security match-policies from-zone zone-A to-zone zone-B source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1004 destination-port 80 protocol tcp result-count 5**

```
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 192.0.2.0/24
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
    Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
  Sequence number: 15
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa11: 10.10.10.1/32
  Destination addresses:
    da15: 192.0.2.5/24
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
    Source port range: [1000-1030]
    Destination port range: [80-80]
```

SEE ALSO

Understanding Security Policy Rules | 106
Understanding Security Policy Elements | 105

Tracking Policy Hit Counts

Use the **show security policies hit-count** command to display the utility rate of security policies according to the number of hits they receive. You can use this feature to determine which policies are being used on the device, and how frequently they are used. Depending on the command options that you choose, the number of hits can be listed without an order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

Checking Memory Usage on SRX Series Devices

Memory for flow entities such as policies, zones, or addresses on SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices (depending on the Junos OS release in your installation) is dynamically allocated. However, certain practices can help monitor the current memory usage on the device and optimize parameters to better size system configuration, especially during policy implementation.

You can isolate memory issues by comparing memory values before and after policy configurations.

To check memory usage:

- Use the **show chassis routing-engine** command to check overall Routing Engine (RE) memory usage. The following output from this command shows memory utilization at 39 percent:

```
user@host# show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    DRAM                       1024 MB
    Memory utilization           39 percent
    CPU utilization:
      User                        0 percent
      Background                  0 percent
      Kernel                      2 percent
      Interrupt                   0 percent
```

```
      Idle                        97 percent
    Model                         RE-PPC-1200-A
    Start time                    2011-07-09 19:19:49 PDT
    Uptime                        37 days, 15 hours, 44 minutes, 13 seconds
    Last reboot reason            0x3:power cycle/failure watchdog
    Load averages:                1 minute   5 minute  15 minute
                                      0.22       0.16       0.07
```

- Use the **show system processes extensive** command to acquire information on the processes running on the Routing Engine.

  Use the **find nsd** option in the **show system processes extensive** command to see direct usage on the Network Security Daemon (NSD) with its total memory in use as 10 megabytes and CPU utilization of 0 percent.

```
user@host# show system processes extensive | find nsd
 1182 root         1  96    0 10976K  5676K select   2:08  0.00% nsd
 1191 root         4   4    0  8724K  3764K select   1:57  0.00% slbd
 1169 root         1  96    0  8096K  3520K select   1:51  0.00% jsrpd
 1200 root         1   4    0     0K    16K peer_s   1:10  0.00% peer proxy
 1144 root         1  96    0  9616K  3528K select   1:08  0.00% lacpd
 1138 root         1  96    0  6488K  2932K select   1:02  0.00% ppmd
 1130 root         1  96    0  7204K  2208K select   1:02  0.00% craftd
 1163 root         1  96    0 16928K  5188K select   0:58  0.00% cosd
 1196 root         1   4    0     0K    16K peer_s   0:54  0.00% peer proxy
   47 root         1 -16    0     0K    16K sdflus   0:54  0.00% softdepflush
 1151 root         1  96    0 15516K  9580K select   0:53  0.00% appidd
  900 root         1  96    0  5984K  2876K select   0:41  0.00% eventd
```

- Check the configuration file size. Save your configuration file with a unique name before exiting the CLI. Then, enter the **ls -1 filename** command from the shell prompt in the UNIX-level shell to check the file size as shown in the following sample output:

```
user@host> start shell
% ls -l config
-rw-r--r--  1 remote  staff  12681 Feb 15 00:43 config
```

SEE ALSO

Best Practices for Defining Policies on SRX Series Devices | 111
Security Policies Overview | 23

Monitoring Security Policy Statistics

Purpose

Monitor and record traffic that Junos OS permits or denies based on previously configured policies.

Action

To monitor traffic, enable the count and log options.

Count—Configurable in an individual policy. If count is enabled, statistics are collected for sessions that enter the device for a given policy, and for the number of packets and bytes that pass through the device in both directions for a given policy. For counts (only for packets and bytes), you can specify that alarms be generated whenever the traffic exceeds specified thresholds. See count (Security Policies).

Log—Logging capability can be enabled with security policies during session initialization (**session-init**) or session close (**session-close**) stage. See log (Security Policies).

- To view logs from denied connections, enable log on **session-init**.
- To log sessions after their conclusion/tear-down, enable log on **session-close**.

> **NOTE:** Session log is enabled at real time in the flow code which impacts the user performance. If both **session-close** and **session-init** are enabled, performance is further degraded as compared to enabling **session-init** only.

For details about information collected for session logs, see *Information Provided in Session Log Entries for SRX Series Services Gateways*.

Verifying Shadow Policies

IN THIS SECTION

- Verifying All Shadow Policies | 267
- Verifying a Policy Shadows One or More Policies | 267
- Verifying a Policy Is Shadowed by One or More Policies | 268

Verifying All Shadow Policies

Purpose

Verify all the policies that shadows one or more policies.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the **show security shadow-policies logical-system *lsys-name* from-zone *from-zone-name* to-zone *to-zone-name*** command.
- For global policies, enter the **show security shadow-policies logical-system *lsys-name* global** command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b

    Policies             Shadowed policies
    P1                   P3
    P1                   P4
    P2                   P5
```

Meaning

The output displays the list of all policies that shadows other policies. In this example, P1 policy shadows P3 and P4 policies and P2 policy shadows P5 policy.

Verifying a Policy Shadows One or More Policies

Purpose

Verify if a given policy shadows one or more policies positioned after it.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the **show security shadow-policies logical-system *lsys-name* from-zone *from-zone-name* to-zone *to-zone-name* policy *policy-name*** command.
- For global policies, enter the **show security shadow-policies logical-system *lsys-name* global policy *policy-name*** command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P1
```

```
Policies              Shadowed policies
 P1                    P3
 P1                    P4
```

Meaning

The output displays all the policies that are shadowed by the given policy. In this example, P1 policy shadows P3 and P4 policies.

Verifying a Policy Is Shadowed by One or More Policies

Purpose

Verify if a given policy is shadowed by one or more positioned before it.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the **show security shadow-policies logical-system *lsys-name* from-zone *from-zone-name* to-zone *to-zone-name* policy *policy-name* reverse** command.
- For global policies, enter the **show security shadow-policies logical-system *lsys-name* global policy *policy-name* reverse** command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse
```

```
Policies              Shadowed policies
 P1                    P4
```

Meaning

The output displays the given policy shadowed by one or more policies. In this example, P4 policy is shadowed by P1 policy.

SEE ALSO

Understanding Security Policy Ordering | 206

Example: Reordering Security Policies | 208

Troubleshooting Security Policies

IN THIS SECTION

- Synchronizing Policies Between Routing Engine and Packet Forwarding Engine | 269
- Checking a Security Policy Commit Failure | 270
- Verifying a Security Policy Commit | 270
- Debugging Policy Lookup | 271

Synchronizing Policies Between Routing Engine and Packet Forwarding Engine

Problem

Description: Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.
- An error with the routing engine, such as a reused policy UID.

Environment: The policies in the Routing Engine and Packet Forwarding Engine must be in sync for the configuration to be committed. However, under certain circumstances, policies in the Routing Engine and the Packet Forwarding Engine might be out of sync, which causes the commit to fail.

Symptoms: When the policy configurations are modified and the policies are out of sync, the following error message displays - **error: Warning: policy might be out of sync between RE and PFE <*SPU-name(s)*> Please request security policies check/resync.**

Solution

Use the **show security policies checksum** command to display the security policy checksum value and use the **request security policies resync** command to synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine, if the security policies are out of sync.

SEE ALSO

show security policies checksum | 541

request security policies check | 490
request security policies resync | 493

Checking a Security Policy Commit Failure

Problem

Description: Most policy configuration failures occur during a commit or runtime.

Commit failures are reported directly on the CLI when you execute the CLI command **commit-check** in configuration mode. These errors are configuration errors, and you cannot commit the configuration without fixing these errors.

Solution

To fix these errors, do the following:

1. Review your configuration data.
2. Open the file /var/log/nsd_chk_only. This file is overwritten each time you perform a commit check and contains detailed failure information.

Verifying a Security Policy Commit

Problem

Description: Upon performing a policy configuration commit, if you notice that the system behavior is incorrect, use the following steps to troubleshoot this problem:

Solution

1. Operational **show** Commands—Execute the operational commands for security policies and verify that the information shown in the output is consistent with what you expected. If not, the configuration needs to be changed appropriately.
2. Traceoptions—Set the **traceoptions** command in your policy configuration. The flags under this hierarchy can be selected as per user analysis of the **show** command output. If you cannot determine what flag to use, the flag option **all** can be used to capture all trace logs.

```
user@host# set security policies traceoptions <flag all>
```

You can also configure an optional filename to capture the logs.

```
user@host# set security policies traceoptions <filename>
```

If you specified a filename in the trace options, you can look in the /var/log/<*filename*> for the log file to ascertain if any errors were reported in the file. (If you did not specify a filename, the default filename is eventd.) The error messages indicate the place of failure and the appropriate reason.

After configuring the trace options, you must recommit the configuration change that caused the incorrect system behavior.

Debugging Policy Lookup

Problem

Description: When you have the correct configuration, but some traffic was incorrectly dropped or permitted, you can enable the **lookup** flag in the security policies traceoptions. The **lookup** flag logs the lookup related traces in the trace file.

Solution

```
user@host# set security policies traceoptions <flag lookup>
```

High Availability (HA) Synchronization of Address Name Resolving Cache

The Network security process (NSD) restarts when system reboots, HA failover happens, or if the process crashes. During this time, if there are large number of domain name addresses configured in the security polices, SRX Series devices attempt to send requests to DNS server to get all resolved IP addresses. A high amount of system resources are consumed when a large number of DNS queries and responses are exchanged. So, SRX Series devices are unable to obtain a response from the DNS server and the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found. The new enhancement on SRX Series devices addresses this problem by caching the DNS query results into a local DNS cache file and periodically synchronizing the DNS cache file from HA primary node to HA backup node. The DNS cache files stores IP addresses, domain name, and TTL values. After the HA failover, the previous backup node becomes primary node. Since all DNS cache results are available on new primary node, security policy processing continues and pass-through traffic is allowed as per the policy rules.

Starting in Junos OS Release 19.3R1, the policy DNS cache memory is synchronized into one local DNS cache file on the HA active node and is copied to the HA backup node to suppress DNS queries or responses during NSD restart.

The following steps are performed for the synchronization to take place:

1. The policy DNS cache memory is synchronized into one local policy DNS cache file located at the */var/db/policy_dns_cache* path every 30 seconds if the policy DNS cache memory content has changed during this period.

2. The local DNS cache file is synchronized from the HA primary node to HA backup node immediately after the local DNS cache file has been updated in Step 1.

The synchronization includes the following content:

- Domain name
- IPv4 address list and its TTL (time to live)
- IPv6 address list and its TTL

When NSD restarts, it reads and parses the local DNS cache file and imports all cache entries into memory. The synchronization ensures that DNS queries are suppressed during an NSD restart. NSD restarts on new primary node during HA failover as the resolved IP addresses for domain names already exist in DNS cache memory when reading policies configurations. Therefore, new pass-through traffic is allowed as per the security policy after HA failover because all resolved IP addresses for domain names exist inside policies on new primary node's Routing Engine and Packet Forwarding Engine.

RELATED DOCUMENTATION

Security Policies Overview | 23

CHAPTER 6

Configuration Statements

address (Security Address Book) | **278**

address-book | **281**

address-set | **283**

alarms (Security) | **284**

alarm-threshold | **286**

alarm-without-drop | **287**

application (Applications) | **288**

application (Security Alarms) | **292**

application (Security Policies) | **293**

application-protocol (Applications) | **295**

application-services (Security Policies) | **297**

application-tracking (Security Zones) | **299**

application-traffic-control (Application Services) | **300**

attach | **301**

audible (Security Alarms) | **302**

authentication (Security Alarms) | **303**

authentication-source (Security) | **304**

captive-portal (Services UAC Policy) | **305**

count (Security Policies) | **306**

default-policy | **307**

deny (Security Policies) | **308**

description (Applications) | **309**

description (Security Address Book) | **310**

description (Security Zone) | **311**

destination-address (Security Policies) | **312**

destination-address (Security Policies Flag) | **313**

destination-address-excluded | **314**

destination-ip (Security Alarms) | **315**

destination-port (Applications) | **317**

dns-cache | **322**

dns-proxy | **324**

dynamic-application (Security) | **326**

dynamic-application (Security Policies) | **328**

dynamic-dns | **330**

exclude (Schedulers) | **331**

firewall-authentication (Security Policies) | **332**

firewall-authentication (User Identification) | **334**

forward-only (DNS) | **335**

from-zone (Security Policies) | **336**

from-zone (Security Policies Global) | **341**

functional-zone | **342**

global (Security Policies) | **344**

host-inbound-traffic | **348**

icmp-code (Applications) | **349**

icmp-type (Applications) | 350

inactivity-timeout (Applications) | 351

interfaces (Security Zones) | 352

initial-tcp-mss | 353

ipsec-group-vpn (Security Policies) | 354

ipsec-vpn (Security Policies) | 355

local-authentication-table | 356

log (Security Policies) | 357

management (Security Zones) | 358

match (Security Policies) | 360

match (Security Policies Global) | 362

unified-policy max-lookups | 364

no-policy-cold-synchronization | 365

pair-policy | 366

pass-through | 367

permit (Security Policies) | 369

policies | 371

policy (Security Alarms) | 382

policy (Security Policies) | 384

policy-match | 388

policy-rematch | 390

policy-stats | 391

potential-violation | 392

pre-id-default-policy | 395

profile(dynamic-application) | 397

protocol (Applications) | 399

protocols (Security Zones Host Inbound Traffic) | 401

protocols (Security Zones Interfaces) | 403

range-address | 405

redirect-wx (Application Services) | 406

reject (Security) | 407

report-skip | 408

reverse-tcp-mss | 409

rpc-program-number (Applications) | 410

scheduler (Security Policies) | 411

scheduler-name | 413

schedulers (Security Policies) | 414

screen (Security Zones) | 415

secure-domains | 416

secure-neighbor-discovery | 417

security-zone | 418

sequence-check-required | 420

services-offload (Security) | 421

session-close | 422

session-init | 423

simple-mail-client-service | 424

source-address (Security Policies) | 425

source-address-excluded | 426

source-identity | 427

source-ip (Security Alarms) | 429

source-port (Applications) | 430

ssl-proxy (Application Services) | 431

ssl-termination-profile | 432

start-date | 433

start-time (Schedulers) | 434

stop-date | 435

stop-time | 436

syn-check-required | 437

system-services (Security Zones Host Inbound Traffic) | 438

system-services (Security Zones Interfaces) | 441

tcp-options (Security Policies) | 443

tcp-rst | 445

term (Applications) | 446

then (Security Policies) | 447

to-zone (Security Policies) | 450

to-zone (Security Policies Global) | 454

traceoptions (dynamic-application) | 455

traceoptions (Security Policies) | 457

traceoptions (Security User Identification) | 459

traceoptions (System Services DNS) | 461

tunnel (Security Policies) | 464

uac-policy (Application Services) | 465

unified-access-control (Security) | 466

unified-policy-explicit-match | 467

user-firewall | 468

user-identification | 470

utm-policy | 472

uuid (Applications) | 474

vrrp | 475

web-authentication | 476

web-redirect | 477

zones | 478

address (Security Address Book)

Syntax

```
address address-name {
    ip-prefix {
        description text;
    }
    description text;
    dns-name domain-name {
        ipv4-only;
        ipv6-only;
    }
    range-address lower-limit to upper-limit;
    wildcard-address ipv4-address/wildcard-mask;
}
```

Hierarchy Level

```
[edit security address-book book-name]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1. Support for address range added in Junos OS Release 12.1. The **description** option added in Junos OS Release 12.1.

Description

Add an entry containing an IP address or DNS hostname, or wildcard address to the address book. An address book contains entries for addressable entities in security zones, policies, and NAT rules. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and DNS names.

Options

- **address *address-name*—**Name of an address entry.
- **description *text*—**Descriptive text about an address entry.
- dns-address ***domain-name*—**DNS address name.
- ***ip-prefix*—**IP address with prefix.
- **range-address *lower-limit* to *upper-limit*—**Address range for an address book.

- **wildcard-address** ***ipv4-address/wildcard-mask***—IPv4 wildcard address in the form of A.B.C.D/wildcard-mask.

> **NOTE:** IPv6 wildcard address configuration is not supported in this release.

Required Privilege Level

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

RELATED DOCUMENTATION

address-book

Syntax

```
address-book (book-name | global) {
    address (Security Address Book) address-name {
        ip-prefix {
            description text;
        }
        description text;
        dns-name domain-name {
            ipv4-only;
            ipv6-only;
        }
        range-address lower-limit to upper-limit;
        wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
        address address-name;
        address-set address-set-name;
        description text;
    }
    attach {
        zone zone-name;
    }
    description (Security Address Book) text;
}
```

Hierarchy Level

```
[edit security]
[edit tenants tenant-name security]
```

Release Information

Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 18.3R1 for tenant systems. Support for wildcard addresses added in Junos OS Release 11.1. Statement moved under the security hierarchy in Junos OS Release 11.2. Support for address range added in Junos OS Release 12.1. The **description** option added in Junos OS Release 12.1.

Description

Define entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range. You define addresses and address

sets in an address book and then use them when configuring different features, such as security policies and NAT.

> **NOTE:** IPv6 wildcard address configuration is not supported in this release.

Options

- **address-book *book-name*—**Name of the address book.
- **global—**An address book that is available by default. You can add any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, DNS names, or address range to the global address book. You do not need to attach the global address book to a security zone; entries in the global address book are available to all security zones that are not attached to address books.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Address Books | 44
Understanding Address Sets | 47

address-set

Syntax

```
address-set address-set-name {
    address address-name;
    address-set address-set-name;
    description text;
}
```

Hierarchy Level

```
[edit security address-book book-name]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for nested address sets introduced in Junos OS Release 11.2. The **description** option added in Junos OS Release 12.1.

Description

Specify a collection of addresses, as defined in the **address (Address Book)** statement. Using address sets, you can organize addresses in logical groups and use them to easily configure other features, such as policies and NAT rules. Using this statement, you can also include a description for an address set.

You can also define address sets within address sets.

Options

***address-set-name*—**Name of the address set.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

alarms (Security)

Syntax

```
alarms {
    audible {
        continuous;
    }
    potential-violation {
        authentication failures;
        cryptographic-self-test;
        decryption-failures {
            threshold value;
        }
        encryption-failures {
            threshold value;
        }
        idp;
        ike-phase1-failures {
            threshold value;
        }
        ike-phase2-failures {
            threshold value;
        }
        key-generation-self-test;
        non-cryptographic-self-test;
        policy {
            application {
                duration interval;
                size count;
                threshold value;
            }
            destination-ip {
                duration interval;
                size count;
                threshold value;
            }
            policy match {
                duration interval;
                size count;
                threshold value;
            }
            source-ip {
                duration interval;
```

```
            size count;
            threshold value;
        }
    }
    replay-attacks {
        threshold value;
    }
    security-log-percent-full percentage;
  }
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configures security alarms.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

alarm-threshold

Syntax

```
alarm-threshold number;
```

Hierarchy Level

```
[edit security screen ids-option screen-name  tcp syn-flood]
```

Release Information

Statement modified in Junos OS Release 9.2.

Description

Define the number of half-complete proxy connections per second at which theSRX300, SRX320, SRX340, SRX345, SRX380, or SRX550M device makes entries in the event alarm log.

Options

number —Threshold value.

Range: 1 through 500,000 per second

Default: 1024 per second

> **NOTE:** For SRX Series devices the applicable range is 1 through 1,000,000 per second.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

alarm-without-drop

Syntax

```
alarm-without-drop;
```

Hierarchy Level

```
[edit security screen ids-option screen-name]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Direct the SRX device to generate an alarm when detecting an attack but not block the attack. Use this statement to allow an attack to enter a segment of your network that you have previously prepared to receive it (for example, a honeynet, which is a decoy network with extensive monitoring capabilities).

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

RELATED DOCUMENTATION

Security Policies Overview | 23

application (Applications)

Syntax

```
application application-name {
    application-protocol (dns | ftp |gprs-gtp-c| gprs-gtp-u | gprs-gtp-v0 |gprs-sctp | http | ignore | ike-esp-nat | mgcp-ca
        | mgcp-ua | ms-rpc | q931 | ras | realaudio | rsh | rtsp | sccp | sip | sqlnet-v2 | sun-rpc | talk | tftp);
    description text;
    destination-port port-identifier;
    do-not-translate-A-query-to-AAAA-query;
    do-not-translate-AAAA-query-to-A-query;
    ether-type hex-value;
    icmp-code value;
    icmp-type value;
    icmp6-code value;
    icmp6-type value;
    inactivity-timeout (seconds | never);
    protocol number;
    rpc-program-number number;
    source-port port-number;
    term term-name {
        alg application;
        destination-port port-identifier;
        icmp-code value;
        icmp-type value;
        icmp6-code value;
        icmp6-type value;
        inactivity-timeout (seconds | never);
        protocol number;
        rpc-program-number number;
        source-port port-number;
        uuid hex-value;
    }
    uuid hex-value;
}
```

Hierarchy Level

```
[edit applications]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Configure application properties at the [applications] hierarchy level.

Options

- **application-protocol *protocol-name***—Specify the name of the application protocol.
- **description *text***—Describe the application.
- **destination-port *port-identifier***—Specify a TCP or UDP destination port number.
- **do-not-translate-A-query-to-AAAA-query**—Set the statement to control the translation of A query to AAAA query.
- **do-not-translate-AAAA-query-to-A-query**—Set the statement to control the translation of AAAA query to A query.
- **ether-type *value***—Specify the Ethernet packet type value.
- **icmp-code *value***—Specify the Internet Control Message Protocol (ICMP) code value.

  Range: 0 through 255.
- **icmp-type *value***—Specify the ICMP packet type value.

  Range: 0 through 255.
- **icmp6-code *value***—Specify the ICMP6 code value.

  Range: 0 through 255.
- **icmp6-type *value***—Specify the ICMP6 packet type value.

  Range: 0 through 255.
- **inactivity-timeout (*seconds* | never)**—Specify the amount of time the application is inactive before it times out in seconds.

  Range: 4 through 129,600 seconds.

  Default: For TCP, 1800 seconds; for UDP, 60 seconds.
- **protocol *value***—Specify the networking protocol name or number.
- **rpc-program-number *value***—Specify the remote procedure call (RPC) or Distributed Computing Equipment (DCE) value.
- **source-port *port-number***—Specify a TCP or UDP source port number.
- **term *term-name***—Specify the individual application protocol.
  - **alg *application***—Specify the name of the application protocol.
  - **destination-port *port-identifier***—Specify a TCP or UDP destination port number.
  - **icmp-code *value***—Specify the ICMP code value.

    Range: 0 through 255.
  - **icmp-type *value***—Specify the ICMP packet type value.

    Range: 0 through 255.

- **icmp6-code *value***—Specify the ICMP6 code value.

  Range: 0 through 255.

- **icmp6-type *value***—Specify the ICMP6 packet type value.

  Range: 0 through 255.

- **inactivity-timeout (*seconds* | never)**—Specify the amount of time the application is inactive before it times out in seconds.

  Range: 4 through 129,600 seconds.

  Default: For TCP, 1800 seconds; for UDP, 60 seconds.

- **protocol *number***—Specify the networking protocol name or number.
- **rpc-program-number *number***—Specify the RPC or DCE value.
- **source-port *port-number***—Specify a TCP or UDP source port number.
- **uuid *hex-vale***—Specify the universal unique identifier (UUID) for objects.

- **uuid *hex-value***—Specify the UUID for objects.

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

RELATED DOCUMENTATION

alg (Applications)

application-protocol (Applications) | **295**

destination-port (Applications) | **317**

application (Security Alarms)

Syntax

```
application {
    duration interval;
    size count;
    threshold value;
}
```

Hierarchy Level

```
[edit security alarms potential-violation policy]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for a number of policy violations to an application within a specified time period.

Options

- **duration *interval***—Indicate the duration of counters.

Range: 1 through 3600 seconds.

Default: 1 second.

- **size *count***—Indicate the number of applications for which policy violation checks can be done concurrently.

Range: 1 through 10240.

Default: 1024.

- **threshold *value***—Indicate the maximum number of application matches required to raise an alarm.

Range: 1 through 4294967295.

Default: 1000.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Security Policies Overview | 23

application (Security Policies)

Syntax

```
application {
    [application];
    any;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

Starting in Junos OS Release 19.1R1, configuring the **application** statement at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]** hierarchy level is optional if the **dynamic-application** statement is configured at the same hierarchy level.

Options

application-name-or-set—Name of the predefined or custom application or application set used as match criteria.

any—Any predefined or custom applications or application sets.

NOTE: A custom application that does not use a predefined destination port for the application will not be included in the **any** option, and must be named explicitly.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Configure Applications in Unified Policies | 165

application-protocol (Applications)

Syntax

```
application-protocol (dns | ftp | http | https | ignore | ike-esp-nat | mgcp-ca | mgcp-ua | ms-rpc | pptp | q931 | ras |
    realaudio | rsh | rtsp | sccp | sip | smtp | sqlnet-v2 | ssh | sun-rpc | talk | telnet | tftp);
```

Hierarchy Level

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

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

Description
Define an application layer gateway (ALG) for a particular application. The following ALGs are supported:

- **dns** —Domain Name Service
- **ftp** —File Transfer Protocol
- **http** —Hypertext Transfer Protocol
- **https** —Hypertext Transfer Protocol
- **ignore** —Ignore application type
- **ike-esp-nat** —IKE ESP NAT application protocol
- **mgcp-ca** —Media Gateway Control Protocol with Call Agent
- **mgcp-ua** —MGCP with User Agent
- **ms-rpc** —Microsoft RPC
- **pptp** —Point-to-Point Tunneling Protocol
- **q931** —ISDN connection control protocol (Q.931)
- **ras** —Remote Access Service
- **realaudio** —RealAudio
- **rsh** —UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp** —Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **smtp** —Simple Mail Transfer Protocol

- **sqlnet-v2** —Oracle SQLNET v2
- **ssh** —Secure Shell Protocol
- **sun-rpc** —Sun Microsystems RPC
- **talk**—TALK program
- **telnet** —Telnet Protocol
- **tftp** —Trivial File Transfer Protocol

Default

If **application-protocol** is not defined, then traffic enters the ALG process as long the status for this ALG is enabled.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

application-services (Security Policies)

Syntax

```
application-services {
    advanced-anti-malware-policy advanced-anti-malware-policy;
    application-firewall {
        rule-set rule-set;
    }
    application-traffic-control {
        rule-set rule-set;
    }
    gprs-gtp-profile gprs-gtp-profile;
    gprs-sctp-profile gprs-sctp-profile;
    idp idp;
    (redirect-wx redirect-wx | reverse-redirect-wx reverse-redirect-wx);
    security-intelligence-policy security-intelligence-policy;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy utm-policy;
    web-proxy {
        profile-name profile-name;
    }
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit]
```

Release Information

Statement modified in Junos OS Release 11.1. The **web-proxy** option is introduced in Junos OS Release 19.2R1.

Description

Enable application services within a security policy. You can enable service such as application firewall, IDP, UTM, SSL proxy, and so on by specifying them in a security policy permit action, when the traffic matches the policy rule.

Options

advanced-anti-malware-policy—Specify advanced-anti-malware policy name.

application-firewall—Specify the rule sets configured as part of application firewall to be applied to the permitted traffic.

application-traffic-control—Specify the rule sets configured as part of AppQoS, application-aware quality of service, to be applied to the permitted traffic.

gprs-gtp-profile—Specify GPRS tunneling protocol profile name.

gprs-sctp-profile—Specify GPRS stream control protocol profile name.

idp—Apply Intrusion detection and prevention (IDP) as application services.

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

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

security-intelligence-policy—Specify security-intelligence policy name.

uac-policy —Enable Unified Access Control (UAC) for the security policy. This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a UAC deployment.

captive-portal *captive-portal*—Specify the preconfigured security policy for captive portal on the Junos OS Enforcer to enable the captive portal feature. The captive portal policy is configured as part of the UAC policy. By configuring the captive portal feature, you can redirect traffic destined for protected resources to the IC Series device or to the URL you configure on the Junos OS Enforcer.

utm-policy *utm-policy*—Specify UTM policy name. The UTM policy configured for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols is attached to the security policy to be applied to the permitted traffic.

web-proxy *profile-name*—Specify secure Web proxy profile name. The secure Web proxy profile is configured with dynamic application and external proxy server details. This profile is attached to the security policy and applied on the permitted traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Application Firewall Overview

application-tracking (Security Zones)

Syntax

```
application-tracking;
```

Hierarchy Level

```
[edit security zones security-zone zone-name]
```

Release Information
Statement introduced in Junos OS Release 10.2.

Description
Enable application tracking support for the zone.

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

RELATED DOCUMENTATION

Example: Configuring Application Tracking

application-traffic-control (Application Services)

Syntax

```
application-traffic-control {
    rule-set rule-set-name;
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services]
[edit logical-systems logical-system-name security policies from-zone zone-name to-zone zone-name policy policy-name
    then permit application-services]
[edit tenants tenant-name security policies from-zone zone-name to-zone zone-name policy policy-name then permit
    application-services]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Support at the following hierarchy levels introduced in Junos OS Release 19.3R1: **[edit logical-systems *logical-system-name* security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]**, and **[edit tenants *tenant-name* security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]**.

Description

Enables AppQoS, application-aware quality of service, as specified in the rules of the specified rule set.

Options

- **rule-set *rule-set-name***—Name of the rule set that contains application-aware traffic control specification rules.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Example: Configuring Application Quality of Service

attach

Syntax

```
attach {
    zone zone-name;
}
```

Hierarchy Level

```
[edit security address-book book-name]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Attach a security zone to an address book. You do not need to attach a security zone to the global address book. The global address book is available by default.

Options

zone *zone-name*—Name of a security zone to be attached to the address book.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Address Books | 44
Understanding Address Sets | 47

audible (Security Alarms)

Syntax

```
audible {
    continuous;
}
```

Hierarchy Level

```
[edit security alarms]
```

Release Information

Statement modified in Junos OS Release 11.2.

Description

Configure alarm to beep when a new security alarm is enabled.

Options

continuous—Specify alarm to keep beeping until all security alarms are cleared.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

authentication (Security Alarms)

Syntax

```
authentication failures;
```

Hierarchy Level

```
[edit security alarms potential-violation]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Raise a security alarm when the device or switch detects a specified number of authentication failures (bad password attempts) before an alarm is raised.

This value must be equal to or less than the **tries-before-disconnect** setting at the **[edit system login retry-options]** hierarchy level; otherwise, the login session ends before the user reaches the alarmable threshold.

Default

Multiple authentication failures do not cause an alarm to be raised.

Options

failures—Number of authentication failures that causes an alarm to be raised.

Range: 1 through 10.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

authentication-source (Security)

Syntax

```
authentication-source {
    active-directory-authentication-table priority priority;
    aruba-clearpass (disable | priority priority);
    firewall-authentication priority priority;
    local-authentication-table priority priority;
    unified-access-control priority priority;
}
```

Hierarchy Level

```
[edit security user-identification]
```

Release Information

Statement introduced in Junos OS Release 12.1. Statement updated in Junos OS Release 12.1-X45-D10. Support for the **active-directory-authentication-table priority** command statement added in Junos OS Release 12.1X47-D10. Statement updated in Junos Release 15.1X49-D60. Support for the **aruba-clearpass** command statement added in Junos OS Release 15.1X49-D60.

Description

Identifies one or more tables to be used as the source for user role information. Tables are searched in sequence based on lowest to highest priority.

> **NOTE:** For arbuba-clearpass, if an entry for the user is not found in the **aruba-clearpass** authentication table, the other authentication tables are searched in the specified order.

Required Privilege Level

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

RELATED DOCUMENTATION

- local-authentication-table | 356
- firewall-authentication (User Identification) | 334
- unified-access-control (Security) | 466

Understanding User Role Firewalls | 183

Understanding the User Identification Table | 186

Understanding Enforcement of ClearPass User and Group Authentication

Example: Enforcing SRX Series Security Policies Using Aruba ClearPass as the Authentication Source

captive-portal (Services UAC Policy)

Syntax

```
captive-portal captive-portal-policy-name;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services
    uac-policy]
```

Release Information

Statement introduced in Junos OS Release 10.2.

Description

Create the captive portal policy in the UAC security policy. You use the captive portal policy to configure the captive portal feature on the Junos OS Enforcer. By configuring the captive portal feature, you can redirect traffic destined for protected resources to the IC Series device or to the URL you configure on the Junos OS Enforcer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

count (Security Policies)

Syntax

```
count;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then]
```

Release Information

Statement introduced in Junos OS Release 8.5. Statement updated in Junos OS Release 12.1X47-D10.

Description

Enable a count, in bytes or kilobytes, of all network traffic the policy allows to pass through the device in both directions: the originating traffic from the client to the server (from the from-zone to the to-zone), and the return traffic from the server to the originating client.

Required Privilege Level

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

RELATED DOCUMENTATION

show security policies | 524
Security Policies Overview | 23

default-policy

Syntax

```
default-policy (deny-all | permit-all);
```

Hierarchy Level

```
[edit security policies]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Configure the default security policy that defines the actions the device takes on a packet that does not match any user-defined policy.

Options
deny-all—Deny all traffic. Packets are dropped. This is the default.

permit-all—Permit all traffic that does not match a policy.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

deny (Security Policies)

Syntax

```
deny;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Block the service at the firewall. The device drops the packets.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

description (Applications)

Syntax

```
description text;
```

Hierarchy Level

```
[edit applications application application-name],
[edit applications application-set application-set-name]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Specify descriptive text for an application or an application set.

> **NOTE:** The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

Options

text—Descriptive text about an application or an application set.

Range: 1 through 300 characters

> **NOTE:** The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

description (Security Address Book)

Syntax

```
description text;
```

Hierarchy Level

```
[edit security address-book book-name]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Specify descriptive text for an address book.

> **NOTE:** The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

Options

text—Descriptive text about an address book.

Range: 1 through 300 characters

> **NOTE:** The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Address Books | 44
Understanding Address Sets | 47

description (Security Zone)

Syntax

```
description text;
```

Hierarchy Level

```
[edit security zones functional-zone management]
[edit security zones security-zone zone-name]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Specify descriptive text for a security zone.

> **NOTE:** The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

Options

text—Descriptive text about a security zone.

Range: 1 through 300 characters

> **NOTE:** The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

destination-address (Security Policies)

Syntax

```
destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information

Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.

Description

Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

Options

address—IP address (**any**, **any-ipv4**, **any-ipv6**), IP address set, or address book entry, or wildcard address (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

destination-address (Security Policies Flag)

Syntax

```
destination-address {
    drop-translated;
    drop-untranslated;
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit]
```

Release Information

Statement introduced in Junos OS Release 9.2.

Description

Specify whether the traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule or to packets where the destination IP address has not been translated.

On Juniper Networks security devices, destination NAT rules are processed before security policy lookup. Therefore, it is possible for a security policy to permit traffic from a source **S** to a destination **D** (where no destination NAT is performed) and also to permit traffic from the source **S** to the destination **d** (where **d** has been translated to **D**).

Options

- **drop-translated**—Drop packets with translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has not been translated.
- **drop-untranslated**—Drop packets without translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

destination-address-excluded

Syntax

```
destination-address-excluded;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name match]
```

Release Information
Statement introduced in Junos OS Release 12.1X45-D10.

Description
Exclude the destination address(es) from the policy.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

destination-ip (Security Alarms)

Syntax

```
destination-ip {
    duration interval;
    size count;
    threshold value;
}
```

Hierarchy Level

```
[edit security alarms potential-violation policy]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for a number of policy violations to a destination network identifier within a specified time period.

Options

- **duration *interval***—Indicate the duration of counters.

Range: 1 through 3600 seconds.

Default: 1 second.

- **size *count***—Indicate the number of destination IP addresses for which policy violation checks can be done concurrently.

Range: 1 through 10240.

Default: 1024.

- **threshold *value***—Indicate the maximum number of destination IP address matches required to raise an alarm.

Range: 1 through 4294967295.

Default: 1000.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

destination-port (Applications)

Syntax

```
destination-port port-identifier;
```

Hierarchy Level

```
[edit applications application application-name],
[edit applications application application-name term term-name]
```

Release Information

Statement modified in Junos OS Release 8.5.

Description

Specify a TCP or UDP destination port number.

Options

port-identifier —Range of ports. You can use a numeric value or one of the text synonyms listed in Table 33 on page 318.

Table 33: Port Supported by Services Interfaces

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

Table 33: Port Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
kpasswd	761
krb-prop	754
krbupdate	760
kshell	544
ldap	389
ldp	646
login	513
mobileip-agent	434
mobilip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723
printer	515
radacct	1813

Table 33: Port Supported by Services Interfaces *(continued)*

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

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

dns-cache

Syntax

```
dns-cache {
    error-response-delete-ip {
        retry-interval seconds;
    }
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name security policies],
[edit logical-systems logical-system-name tenants tenant-system-name security policies],
[edit security policies],
[edit tenants tenant-system-name security policies]
```

Release Information

Statement introduced in Junos OS Release 20.1R1.

Description

Define security policy DNS cache behaviors. The following behaviors can occur:

- Flushing of the DNS cache entry on error response.
- Keeping the DNS cache entry unchanged on all DNS servers time out.
- Updating the DNS cache entry when there is a positive response.

Options

error-response-delete-ip—Clear DNS cache entry IP on error DNS response

Values:

retry-interval—Interval between deleting IP and resending DNS requests

Range: 5 through 86400 seconds.

Default: 300 seconds.

Required Privilege Level

security

RELATED DOCUMENTATION

show security dns-cache

clear security dns-cache

dns-proxy

Syntax

```
dns-proxy {
    cache hostname inet ip-address;
    default-domain domain-name {
        forwarders ip-address;
    }
    interface interface-name;
    propogate-setting (enable | disable);
    view view-name {
        domain domain-name {
            forward-only;
            forwarders ip-address;
        }
        match-clients subnet-address;
    }
}
```

Hierarchy Level

```
[edit system services dns dns-proxy]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Description

Configure the device as a DNS proxy server by enabling DNS proxy on a logical interface. This option is supported on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

DNS Proxy Overview

dynamic-application (Security)

Syntax

```
dynamic-application {
    profile profile name {
        redirect-message {
            type {
                custom-text {
                    content content;
                }
                redirect-url {
                    content content;
                }
            }
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 18.2R1.

Description

Configure options for dynamic applications to define a redirect profile and traceoptions.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Example: Configure a Unified Policy Using a Redirect Message Profile | **154**

Unified Policies Configuration Overview | **146**

dynamic-application (Security Policies)

Syntax

```
dynamic-application;
```

Hierarchy Level

```
[edit security policies from-zone zone-name policy policy-name match]
[edit security policies global policy policy-name match]
```

Release Information
Statement introduced in Junos OS Release 18.2R1.

Description
Specify the dynamic applications or dynamic application groups used as match criteria within a security policy.

By adding dynamic applications to the match criteria, the data traffic is classified based on the Layer 7 application inspection results. Application Identification (AppID) identifies dynamic or real-time Layer 4 through Layer 7 applications. After a particular application is identified and the matching policy is found, then the actions are applied according to the policy.

Options

dynamic-application-name* |*dynamic-application-group-name—Specify dynamic applications or dynamic application groups.

Examples for dynamic applications or dynamic application groups are as follows:

- **junos:FTP** (dynamic application)
- **junos:web:shopping** (dynamic application group)

any—Configuring the dynamic application as **any** installs the policy with the application as a wildcard (default). If an application cannot be specified, configure **any** as the default application. Data traffic that match the parameters in a unified policy matches the policy regardless of the application type.

none—Configuring the dynamic application as **none** ignores classification results from AppID and does not use the dynamic application in security policy lookups. Within the list of potential match policies, if there is any policy configured with dynamic application as **none**, this policy is matched as the final policy and is terminal. If any Layer 7 services are configured in this policy, deep packet inspection for the traffic is performed.

When upgrading the Junos OS release from previous releases (where dynamic applications were not supported), all existing traditional policies are considered as policies with the dynamic application configured as **none**.

If dynamic application is not configured within a security policy, the policy is considered to be a traditional security policy. This policy is similar to a policy with the dynamic application configured as **none**.

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

RELATED DOCUMENTATION

Unified Policies Overview | **145**

Unified Policies Configuration Overview | **146**

dynamic-dns

Syntax

```
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password server-password;
        server server-name;
        username user-name;
    }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Description

Configure the device as a dynamic DNS server that maintains the list of the changed addresses and their associated domain names registered with it. The device updates these DDNS servers with this information periodically or whenever there is a change in IP addresses.

Options

- **client** —Specifies the hostname of the registered client.
- **agent**—Specifies the name of the dynamic DNS agent.
- **interface** —Specifies the interface whose IP address is mapped to the registered domain name.
- **password**—Specifies the password.
- **server**—Specifies the name of the dynamic DNS server that allows dynamic DNS clients to update the IP address changes associated with the registered hostname.
- **username**—Specifies the dynamic DNS username.

Required Privilege Level

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

RELATED DOCUMENTATION

DNS Overview

exclude (Schedulers)

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 Junos OS Release 8.5.

Description
Exclude a specified day from the schedule.

Use the **exclude** statement to exclude a day from a daily schedule created with the **daily** statement. You cannot use the **exclude** statement for a particular day unless it is in conjunction with the **daily** statement in a schedule.

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

RELATED DOCUMENTATION

Security Policy Schedulers Overview | 210

firewall-authentication (Security Policies)

Syntax

```
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
        auth-only-browser
            auth-user-agent
    }
    push-to-identity-management
    user-firewall {
        access-profile profile-name;
        domain domain-name
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
        auth-only-browser
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information

Statement introduced in Junos OS Release 8.5.

Support added for the **user-firewall** option in Junos OS Release 12.1X45-D10.

Support for the **ssl-termination-profile** and **web-redirect-to-https** options added on SRX5600 and SRX5800 Services Gateways starting from Junos OS Release 12.1X44-D10, on SRX5400 devices starting from 12.1X46-D10, and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.

Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, support for the **web-redirect** and **web-redirect-to-https** options under **user-firewall** added on SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX Services Gateways.

Starting with Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, support for the **auth-only-browser** option was added under **pass-through** and **user-firewall** and the **auth-user-agent** option was added under **pass-through auth-only-browser** on SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX Services Gateways.

Starting with Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, support for the **auth-only-browser** option was added under **pass-through** and **user-firewall** and the **auth-user-agent** option was added under **pass-through auth-only-browser** on SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX Services Gateways. Starting with Junos OS Release 15.1X49-D100 and Junos OS Release 17.3R1, support was added for **push-to-identity-management**.

Description

Configure firewall authentication methods.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

firewall-authentication (User Identification)

Syntax

```
firewall-authentication priority priority;
```

Hierarchy Level

```
[edit security user-identification authentication-source]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10. Support for **disable** option dropped in Junos OS Release 12.1X47-D10.

Description

Enables the firewall authentication table as an authentication source. The priority of this table among other authentication tables establishes the search sequence used to identify user and role values.

Options

priority—A unique value between 0 and 65535 that determines the sequence for searching multiple tables to retrieve a user role. Each table is given a unique priority value. The lower the value, the higher the priority. A table with priority 120 is searched before a table with priority 200.

Default: 150

Setting the priority value of the firewall authentication table to 0 is equivalent to disabling the table and eliminating it from the search sequence.

Required Privilege Level

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

RELATED DOCUMENTATION

authentication-source (Security) | 304

Understanding User Role Firewalls | 183

forward-only (DNS)

Syntax

```
forward-only;
```

Hierarchy Level

```
[edit system services dns dns-proxy view view-name domain domain-name]
```

Release Information
Statement introduced in Junos OS Release 12.1X46-D10.

Description
Specify that the server to forward only DNS queries. This configuration prevents the device from acquiring public IP addresses, in case the IP address specified in **forwarders** option is not reachable, by terminating the DNS query.

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

RELATED DOCUMENTATION

- *DNS Overview*

from-zone (Security Policies)

Syntax

```
from-zone zone-name to-zone zone-name {
    policy policy-name {
        description description;
        match {
            application {
                [junos-defaults | application];
                any;
                junos-smtps;
                junos-imaps;
                junos-pop3s;
                }
            }
            dynamic-application {
                [dynamic-application-name |dynamic-application-group-name];
                any;
                none;
            }
            destination-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-identity {
                [role-name];
                any;
                authenticated-user;
                unauthenticated-user;
                unknown-user;
            }
            source-end-user-profile {
                profile-name;
            }
        }
```

```
scheduler-name scheduler-name;
```

```
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
                profile-name profile-name;
            }
            uac-policy {
                captive-portal captive-portal;
            }
            utm-policy policy-name;
        }
        destination-address {
            drop-translated;
            drop-untranslated;
        }
        firewall-authentication {
            pass-through {
                access-profile profile-name;
                client-match user-or-group-name;
                ssl-termination-profile profile-name;
                web-redirect;
                web-redirect-to-https;
            }
```

```
            user-firewall {
               access-profile profile-name;
               domain domain-name
               ssl-termination-profile profile-name;
            }
            web-authentication {
               client-match user-or-group-name;
            }
         }
         services-offload;
         tcp-options {
            initial-tcp-mss mss-value;
            reverse-tcp-mss mss-value;
            sequence-check-required;
            sequence-check-required;
            syn-check-required;
         }
         tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
         }
      }
      deny | reject;
      deny | reject [profile name];
   }
  }
}
```

Hierarchy Level

```
[edit security policies]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **description** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **dynamic-application** and **deny** options added in Junos OS Release 18.2R1.

Description

Specify a source zone and destination zone to be associated with the security policy.

Options

- **from-zone *zone-name***—Name of the source zone.
- **to-zone *zone-name***—Name of the destination zone.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | **23**
- Understanding Security Policy Rules | **106**
- Understanding Security Policy Elements | **105**
- Unified Policies Configuration Overview | **146**

from-zone (Security Policies Global)

Syntax

```
from-zone {
    [zone-name];
    any;
}
```

Hierarchy Level

```
[edit security policies global policy policy-name match]
```

Release Information

Statement introduced in Junos OS Release 12.1X47-D10.

Description

Identify a single source zone or multiple source zones to be used as a match criteria for a policy. You must configure specific zones or default to any zone, but you cannot have both in a global policy.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

functional-zone

Syntax

```
functional-zone {
    management {
        description text;
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
        interfaces interface-name  {
            host-inbound-traffic {
                protocols protocol-name {
                    except;
                }
                system-services service-name {
                    except;
                }
            }
        }
        screen screen-name;
    }
}
```

Hierarchy Level

```
[edit security zones]
```

Release Information

Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1.

Description

Configure a functional zone.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Understanding Functional Zones*

global (Security Policies)

Syntax

```
global {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
            destination-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            from-zone {
                [zone-name];
                any;
            }
            source-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-identity {
                [role-name];
                any;
                authenticated-user;
                unauthenticated-user;
                unknown-user;
            }
                to-zone {
                    [zone-name];
                    any;
                }
        }
        scheduler-name scheduler-name;
        then {
            count {
                alarm {
```

```
        per-minute-threshold number;
        per-second-threshold number;
    }
}
deny;
log {
    session-close;
    session-init;
}
```

```
        permit {
            application-services {
                application-firewall {
                    rule-set rule-set-name;
                }
                application-traffic-control {
                    rule-set rule-set-name;
                }
                gprs-gtp-profile profile-name;
                gprs-sctp-profile profile-name;
                idp;
                redirect-wx | reverse-redirect-wx;
                ssl-proxy {
                    profile-name profile-name;
                }
                uac-policy {
                    captive-portal captive-portal;
                }
                utm-policy policy-name;
            }
            destination-address {
                drop-translated;
                drop-untranslated;
            }
            firewall-authentication {
                pass-through {
                    access-profile profile-name;
                    client-match user-or-group-name;
                    web-redirect;
                }
                web-authentication {
                    client-match user-or-group-name;
                }
            }
            services-offload;
            tcp-options {
                sequence-check-required;
                syn-check-required;
            }
        }
        reject;
    }
  }
}
```

Hierarchy Level

[edit security policies]

Release Information

Statement introduced in Junos OS Release 8.5. Statement updated with **from-zone** and **to-zone** policy match options in Junos OS Release 12.1X47-D10.

Description

Configure a global policy.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Global Policy Overview | **172**

host-inbound-traffic

Syntax

```
host-inbound-traffic {
    protocols protocol-name {
        except;
    }
    system-services 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 Junos OS Release 8.5.

Description

Control the type of traffic that can reach the device from interfaces bound to the zone.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding How to Control Inbound Traffic Based on Traffic Types | 33

Understanding How to Control Inbound Traffic Based on Protocols | 37

icmp-code (Applications)

Syntax

```
icmp-code value;
```

Hierarchy Level

```
[edit applications application application-name  ]
[edit applications application application-name  term  term-name]
```

Release Information
Statement modified in Junos OS Release 8.5.

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

Options
value — Specify the Internet Control Message Protocol (ICMP) code value such as **host-unreachable** or **host-unreachable-for-tos**.

Range: 0 through 255.

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

icmp-type (Applications)

Syntax

```
icmp-type value;
```

Hierarchy Level

```
[edit applications application application-name  ]
[edit applications application application-name  term  term-name]
```

Release Information

Statement modified in Junos OS Release 8.5.

Description

Specify the ICMP packet type value.

Options

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

Range: 0 through 255.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

inactivity-timeout (Applications)

Syntax

```
inactivity-timeout (seconds | never) ;
```

Hierarchy Level

```
[edit applications application application-name  ]
[edit applications application application-name  term  term-name]
```

Release Information
Statement modified in Junos OS Release 8.5.

Description
Inactivity timeout period, in seconds.

Options
seconds—Specify the amount of time the application is inactive before it times out in seconds.

Range: 4 through 86400 seconds.

Default: For TCP, 1800 seconds; for UDP, 60 seconds.

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

interfaces (Security Zones)

Syntax

```
interfaces interface-name {
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
}
```

Hierarchy Level

```
[edit security zones functional-zone management],
[edit security zones security-zone zone-name]
```

Release Information

Statement introduced in Junos OS Release 8.5.

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. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Security Zones | 29

initial-tcp-mss

Syntax

```
initial-tcp-mss mss-value;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit tcp-options]
```

Release Information
Statement introduced in Junos OS Release 12.3X48-D20.

Description
Configure the TCP maximum segment size (MSS) for packets that arrive at the ingress interface (initial direction), match a specific policy, and for which a session is created. The value you configure overrides the TCP MSS value in the incoming packet when the value in the packet is higher than the one you specify.

The **initial-tcp-mss** value per policy takes precedence over a global **tcp-mss** value (**all-tcp**, **ipsec-vpn**, **gre-in**, **gre-out**), if one is configured. However, when the **syn-flood-protection-mode syn-proxy** statement at the **[edit security flow]** hierarchy level is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overriden.

Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure a TCP MSS value for the reverse session, use the **reverse-tcp-mss** option.

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

RELATED DOCUMENTATION

reverse-tcp-mss | 409

tcp-mss (Security Flow)

syn-flood-protection-mode

ipsec-group-vpn (Security Policies)

Syntax

```
ipsec-group-vpn group-vpn;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit tunnel]
```

Release Information

Statement introduced in Junos OS Release 10.2.

Description

Specify group VPN tunnel for the traffic configured by the scope policy on a group member.

Options

group-vpn —Name of the group VPN tunnel configured on the group member.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | 23
- *Group VPNv2 Overview*
- Security Basics Overview | 23

ipsec-vpn (Security 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 Junos OS Release 8.5.

Description
Define IPsec name for VPN.

Options
vpn-name —Name of the IPsec.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

local-authentication-table

Syntax

```
local-authentication-table priority priority;
```

Hierarchy Level

```
[edit security user-identification authentication-source]
```

Release Information

Statement introduced in Junos OS Release 12.1. Support for **disable** option dropped in Junos OS Release 12.1X47-D10.

Description

An authentication table created on the SRX Series device using the **request security user-identification local-authentication-table add** command.

Options

priority *priority*—A unique value between 0 and 65535 that determines the sequence for searching multiple tables to retrieve a user role. Each table is given a unique priority value. The lower the value, the higher the priority. A table with priority 120 is searched before a table with priority 200. The default priority value of the local authentication table is 100.

Setting the priority value of the local authentication table to 0 is equivalent to disabling the table and eliminating it from the search sequence.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

Understanding the User Identification Table | 186

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 Junos OS Release 8.5.

Description

Log traffic information for a specific policy. Traffic information is logged when a session begins (session-init) or closes (session-close).

> **NOTE:** You must configure security policy for the session using the **set security policies from-zone zone-name to-zone zone-name policy *policy-name* then log session-close** command to list all the applications and nested applications in Application Tracking on J-Web using the on-box reporting feature.

Options

session-close—Start logging traffic when the session ends.

session-init—Start logging traffic when the session begins.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding On-Box Logging and Reporting

Example: Configuring Application Tracking

management (Security Zones)

Syntax

```
management {
    description text;
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
    interfaces interface-name  {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
}
```

Hierarchy Level

```
[edit security zones functional-zone]
```

Release Information

Statement introduced in Junos OS Release 8.5.The **description** option added in Junos OS Release 12.1.

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 originate from any other zone.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Security Zones Overview | 27

Understanding Functional Zones

match (Security Policies)

Syntax

```
match {
    application {
        [application];
        any;
    }
    destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
    }
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

Release Information

Statement introduced in Junos OS Release 8.5. Statement updated with the **source-identity** option in Junos OS Release 12.1.

Description

Configure security policy match criteria.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Security Policies Overview | 23

match (Security Policies Global)

Syntax

```
match {
    application {
        [application];
        any;
    }
    destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    from-zone {
        [zone-name];
        any;
    }
    source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
    }
    source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
    }
    to-zone {
        [zone-name];
        any;
    }
}
```

Hierarchy Level

```
[edit security policies global policy policy-name]
```

Release Information

Statement modified in Junos OS Release 8.5. Statement updated with **source-identity** option in Junos OS Release 12.1. Statement updated with **to-zone** and **from-zone** options in Junos OS Release 12.1X47-D10.

Description

Configure security global policy match criteria.

> **NOTE:** We recommend that, for security reasons and to avoid spoofing traffic, when you create a multizone policy you use identical matching criteria (source address, destination address, application) and an identical action. For more information see "Global Policy Overview" on page 172.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

unified-policy max-lookups

Syntax

```
unified-policy max-lookups max-lookups-number;
```

Hierarchy Level

```
[edit logical-systems name security policies],
[edit logical-systems name tenants name security policies],
[edit security policies]
[edit tenants tenant-name security policies]
```

Release Information

Statement introduced in Junos OS Release 19.2R1.

Description

Configure maximum number of policy lookups, when micro-applications reach the *transaction final* state, during the dynamic application classification process.

Application classification with micro-applications does not reach the *final match* state because the micro-application keeps changing for the session. When the micro-application changes from one transaction to another, a policy lookup is attempted unlimited number of times. The *final match* state for the application is required for the policy lookup and for processing the policy. You can limit the number of transactions for the micro application by configuring the **unified-policy max-lookups** statement.

Setting the value of **unified-policy max-lookups** as 0 indicates unlimited number of policy lookups.

Range: 0 through 25

Default

The default value for **unified-policy max-lookups** is 2.

Required Privilege Level

flow-tap

RELATED DOCUMENTATION

Configure Micro-Applications in Unified Policies | 170

no-policy-cold-synchronization

Syntax

no-policy-cold-synchronization

Hierarchy Level

[edit security idp sensor-configuration high-availability]

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Disable policy cold synchronization functionality. This prevents the SRX Series devices from waiting for the IPS policy to be loaded on all service PICs, and there by forfeits IPS service protection during the ISSU (In-service software upgrade) operation/window.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

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 Junos OS Release 8.5.

Description
Link the policy that you are configuring with another policy that references the same VPN tunnel so that both policies share one proxy ID and one security association (SA). Policy pairing is useful when you want to allow bidirectional traffic over a policy-based VPN that is using source or destination address translation with a dynamic IP address pool or destination address translation with a mapped IP (MIP) or dynamic IP (DIP) address pool.

Without policy pairing, the device derives a different proxy ID from the outbound and inbound policies. Two proxy IDs causes a problem for the remote peer with a single proxy ID for the VPN tunnel.

Pairing two policies solves the proxy ID problem for the remote peer and conserves SA resources. The single proxy ID is derived from the policy you configured last.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

pass-through

Syntax

```
pass-through {
    access-profile profile-name;
    client-match user-or-group-name;
    ssl-termination-profile profile-name;
    web-redirect;
    web-redirect-to-https;
}
```

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 Junos OS Release 8.5. Support for **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

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) Specify the name of the access profile.
- **client-match** ***user-or-group*** —(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.
- **ssl-termination-profile** ***profile-name*** —(Optional) Specify the SSL termination profile used for SSL offloading.
- **web-redirect**—(Optional) Enable redirecting an HTTP request to the device and redirecting the client system to a webpage for authentication. Including this statement allows users an easier authentication process because they need to know only the name or IP address of the resource they are trying to access.
- **web-redirect-to-https**—(Optional) Redirect unauthenticated HTTP requests to the internal HTTPS Web server of the device.

> **NOTE:** If **web-redirect-to-https** is set, then you must specify the SSL termination profile used for SSL offloading.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Security Policies Overview | 23

permit (Security Policies)

Syntax

```
permit {
    application-services {
        application-firewall {
            rule-set rule-set-name;
        }
        application-traffic-control {
            rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
        uac-policy {
            captive-portal captive-portal;
        }
        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            ssl-termination-profile profile-name;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile profile-name;
            domain domain-name
            ssl-termination-profile profile-name;
        }
        web-authentication {
            client-match user-or-group-name;
        }
```

```
    }
    services-offload;
    tcp-options {
        sequence-check-required;
        syn-check-required;
    }
    tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
        pair-policy pair-policy;
    }
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **tcp-options** added in Junos OS Release 10.4. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.

Description

Specify the policy action to perform when packets match the defined criteria.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

policies

Syntax

```
policies {
    default-policy (deny-all | permit-all);
    from-zone from-zone-name {
        to-zone;
        policy name {
            description description;
            match (Security Policies Global) {
                source-address (Security Policies);
                destination-address (Security Policies);
                application (Security Policies);
                source-identity;
                source-end-user-profile <source-end-user-profile-name>;
                dynamic-application (Security Policies);
                url-category;
                from-zone (Security Policies Global);
                to-zone (Security Policies Global);
                source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
                destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
                destination-address-excluded;
                source-address-excluded;
            }
            scheduler-name scheduler-name;
            then {
                deny;
                permit {
                    application-services {
                        (redirect-wx | reverse-redirect-wx);
                        advanced-anti-malware-policy advanced-anti-malware-policy;
                        application-traffic-control {
                            rule-set rule-set;
                        }
                        gprs-gtp-profile gprs-gtp-profile;
                        gprs-sctp-profile gprs-sctp-profile;
                        icap-redirect icap-redirect;
                        idp;
                        idp-policy idp-policy;
                        security-intelligence-policy security-intelligence-policy;
                        ssl-proxy {
                            profile-name profile-name;
                        }
```

```
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy utm-policy;
    web-proxy {
        profile-name profile-name;
    }
}
destination-address {
    (drop-translated | drop-untranslated);
}
firewall-authentication {
    pass-through {
        access-profile access-profile;
        auth-only-browser;
        auth-user-agent name;
        client-match [ client-match ... ];
        ssl-termination-profile ssl-termination-profile;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile access-profile;
        auth-only-browser;
        auth-user-agent name;
        domain domain;
        ssl-termination-profile ssl-termination-profile;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match [ client-match ... ];
    }
    push-to-identity-management;
}
services-offload;
tcp-options {
    initial-tcp-mss initial-tcp-mss;
    reverse-tcp-mss reverse-tcp-mss;
    sequence-check-required;
    syn-check-required;
    window-scale;
}
```

```
            tunnel {
                ipsec-vpn ipsec-vpn;
                pair-policy pair-policy;
            }
        }
        reject {
            profile profile;
            ssl-proxy {
                profile-name profile-name;
            }
        }
        count {
        }
        log {
            session-close;
            session-init;
        }
    }
  }
}
```

```
global {
    policy name {
        description description;
        match (Security Policies Global) {
            source-address (Security Policies);
            destination-address (Security Policies);
            application (Security Policies);
            source-identity;
            source-end-user-profile <source-end-user-profile-name>;
            dynamic-application (Security Policies);
            url-category;
            from-zone (Security Policies Global);
            to-zone (Security Policies Global);
            source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
            destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
            destination-address-excluded;
            source-address-excluded;
        }
        scheduler-name scheduler-name;
        then {
            deny;
            permit {
                application-services {
                    (redirect-wx | reverse-redirect-wx);
                    advanced-anti-malware-policy advanced-anti-malware-policy;
                    application-traffic-control {
                        rule-set rule-set;
                    }
                    gprs-gtp-profile gprs-gtp-profile;
                    gprs-sctp-profile gprs-sctp-profile;
                    icap-redirect icap-redirect;
                    idp;
                    idp-policy idp-policy;
                    security-intelligence-policy security-intelligence-policy;
                    ssl-proxy {
                        profile-name profile-name;
                    }
                    uac-policy {
                        captive-portal captive-portal;
                    }
                    utm-policy utm-policy;
                    web-proxy {
                        profile-name profile-name;
                    }
```

```
    }
    destination-address {
        (drop-translated | drop-untranslated);
    }
    firewall-authentication {
        pass-through {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            client-match [ client-match ... ];
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            domain domain;
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match [ client-match ... ];
        }
        push-to-identity-management;
    }
    services-offload;
    tcp-options {
        initial-tcp-mss initial-tcp-mss;
        reverse-tcp-mss reverse-tcp-mss;
        sequence-check-required;
        syn-check-required;
        window-scale;
    }
    tunnel {
        ipsec-vpn ipsec-vpn;
        pair-policy pair-policy;
    }
}
```

```
            reject {
                profile profile;
                ssl-proxy {
                    profile-name profile-name;
                }
            }
            count {
            }
            log {
                session-close;
                session-init;
            }
        }
    }
}
policy-rematch <extensive>;
policy-stats {
    system-wide (disable | enable);
}
pre-id-default-policy {
    then {
        log {
            session-close;
            session-init;
        }
        session-timeout {
            icmp seconds;
            icmp6 seconds;
            ospf seconds;
            others seconds;
            tcp seconds;
            udp seconds;
        }
    }
}
```

```
stateful-firewall-rule name {
    match-direction (input | input-output | output);
    policy name {
        description description;
        match (Security Policies Global) {
            source-address (Security Policies);
            destination-address (Security Policies);
            application (Security Policies);
            source-identity;
            source-end-user-profile <source-end-user-profile-name>;
            dynamic-application (Security Policies);
            url-category;
            from-zone (Security Policies Global);
            to-zone (Security Policies Global);
            source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
            destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
            destination-address-excluded;
            source-address-excluded;
        }
        scheduler-name scheduler-name;
        then {
            deny;
            permit {
                application-services {
                    (redirect-wx | reverse-redirect-wx);
                    advanced-anti-malware-policy advanced-anti-malware-policy;
                    application-traffic-control {
                        rule-set rule-set;
                    }
                    gprs-gtp-profile gprs-gtp-profile;
                    gprs-sctp-profile gprs-sctp-profile;
                    icap-redirect icap-redirect;
                    idp;
                    idp-policy idp-policy;
                    security-intelligence-policy security-intelligence-policy;
                    ssl-proxy {
                        profile-name profile-name;
                    }
                    uac-policy {
                        captive-portal captive-portal;
                    }
                    utm-policy utm-policy;
                    web-proxy {
                        profile-name profile-name;
```

```
        }
    }
    destination-address {
        (drop-translated | drop-untranslated);
    }
    firewall-authentication {
        pass-through {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            client-match [ client-match ... ];
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            domain domain;
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match [ client-match ... ];
        }
        push-to-identity-management;
    }
    services-offload;
    tcp-options {
        initial-tcp-mss initial-tcp-mss;
        reverse-tcp-mss reverse-tcp-mss;
        sequence-check-required;
        syn-check-required;
        window-scale;
    }
    tunnel {
        ipsec-vpn ipsec-vpn;
        pair-policy pair-policy;
    }
}
```

```
            reject {
                profile profile;
                ssl-proxy {
                    profile-name profile-name;
                }
            }
            count {
            }
            log {
                session-close;
                session-init;
            }
        }
    }
}
stateful-firewall-rule-set name {
    stateful-firewall-rule name;
}
traceoptions (Security Policies) {
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
    flag name;
    no-remote-trace;
}
unified-policy {
    max-lookups max-lookups;
}
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Support for the **services-offload** option added in Junos OS Release 11.4.
Support for the **source-identitiy** option added in Junos OS Release 12.1.
Support for the **description** option added in Junos OS Release 12.1.
Support for the **ssl-termination-profile** and **web-redirect-to-https** options are added starting from Junos OS Release 12.1X44-D10 and Junos OS Release 15.1X49-D40.
Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.
Support for the **domain** option, and for the **from-zone** and **to-zone** global policy match options, added in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.
Support for the **extensive** option for **policy-rematch** added in Junos OS Release 15.1X49-D20.
Starting in Junos OS Release 18.2R1, an IDP policy is available within unified security policy. The IDP policy access is simplified and made available under the unified policy as one of the policy. When an IDP policy is available within a unified security policy, configuring source or destination address, source and destination-except, from and to zone, or application is not required, because the match happens in the security policy itself.
Starting in Junos OS Release 18.3R1, when an SRX Series device is configured with a unified policies, you can configure multiple IDP policies and set one of those policies as the default IDP policy. If multiple IDP policies are configured for a session and when policy conflict occurs, the device applies the default IDP policy for that session and thus resolves any policy conflicts.

> **NOTE:** If you have configured two or more IDP policies in a unified security policy, then you must configure the default IDP policy.

Description

Configure a network security policies with IPv6 addresses only if flow support for IPv6 traffic is enabled on the device.

Options

default-policy—Configure a default action when no user-defined policy match.

Values:

- deny-all—Deny all traffic if no policy match
- permit-all—Permit all traffic if no policy match

policy-rematch—Re-evaluate the policy when changed.

Values:

- extensive—Perform policy extensive rematch

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

policy (Security Alarms)

Syntax

```
policy {
    application {
        duration interval;
        size count;
        threshold value;
    }
    destination-ip {
        duration interval;
        size count;
        threshold value;
    }
    policy match {
        duration interval;
        size count;
        threshold value;
    }
    source-ip {
        duration interval;
        size count;
        threshold value;
    }
}
```

Hierarchy Level

```
[edit security alarms potential-violation]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for policy violation, based on source IP, destination IP, application, and policy rule.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

policy (Security Policies)

Syntax

```
policy policy-name {
    description description;
    match {
        application {
            [application];
            any;
            junos-twamp;
        }
        destination-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
        }
        source-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
        }
        source-identity {
            [role-name];
            any;
            authenticated-user;
            unauthenticated-user;
            unknown-user;
        }
    }
    scheduler-name scheduler-name;
    then {
        count {
            alarm {
                per-minute-threshold number;
                per-second-threshold number;
            }
        }
        deny;
        log {
            session-close;
            session-init;
```

```
    }
```

```
permit {
    application-services {
        application-firewall {
            rule-set rule-set-name;
        }
        application-traffic-control {
            rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
        uac-policy {
            captive-portal captive-portal;
        }
        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            web-redirect;
        }
        user-firewall {
            access-profile profile-name;
            domain domain-name
            ssl-termination-profile profile-name;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        initial-tcp-mss mss-value;
        reverse-tcp-mss mss-value;
        sequence-check-required;
```

```
            syn-check-required;
        }
        tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
        }
    }
    reject;
  }
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name]
```

Release Information

Statement introduced in Junos OS Release 8.5. The **services-offload** option added in Junos OS Release 11.4. Statement updated with the **source-identity** option and the **description** option added in Junos OS Release 12.1. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.
The **junos-twamp** application is introduced in Junos OS Release 18.2R1.

Description

Define a security policy.

Options

policy-name—Name of the security policy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SSL Forward Proxy

policy-match

Syntax

```
policy match {
    duration interval;
    size count;
    threshold value;
}
```

Hierarchy Level

```
[edit security alarms potential-violation policy]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for a policy rule or a group of rule violations within a specified time period.

Options

- **duration *interval***—Indicate the duration of counters.

Range: 1 through 3600 seconds.

Default: 1 second.

- **size *count***—Indicate the number of policies for which policy violation checks can be done concurrently.

Range: 1 through 10240.

Default: 1024.

- **threshold *value***—Indicate the number of policies for which policy violation checks can be done concurrently.

Range: 1 through 4294967295.

Default: 1000.

Required Privilege Level

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

RELATED DOCUMENTATION

policy-rematch

Syntax

```
policy-rematch extensive;
```

Hierarchy Level

```
[edit security policies]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **extensive** option added in Junos OS Release 15.1X49-D20.

Description

Enable the device to reevaluate an active session when its associated security policy is modified. The session remains open if it still matches the policy that allowed the session initially.

The session is closed if its associated policy is renamed, deactivated, or deleted. However, you can use the **extensive** option to reevaluate an active session when its associated security policy is renamed, deactivated, or deleted.

The policy rematch feature is disabled by default.

Options

extensive—Enable the device to reevaluate an active session when its associated security policy is modified, renamed, deactivated, or deleted. The session remains active if it matches another policy that allows the session.

NOTE: The **extensive** option does not apply to ALG data sessions or to policies that specify a source-identity, application-services, destination-address (drop-untranslated or drop-translated), firewall-authentication, or a tunnel.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23
Unified Policies Configuration Overview | 146

policy-stats

Syntax

```
policy-stats {
    system-wide (disable | enable) ;
}
```

Hierarchy Level

```
[edit security policies]
```

Release Information

Statement introduced in Junos OS Release 12.1X46-D10.

Description

Configure systemwide policies statistics. The systemwide policies statistics are disabled by default.

Options

disable—Disable systemwide policy statistics.

enable—Enable systemwide policy statistics.

Required Privilege Level

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

RELATED DOCUMENTATION

show security policies | 524

potential-violation

Syntax

```
potential-violation {
    authentication failures;
    cryptographic-self-test;
    decryption-failures {
        threshold value;
    }
    encryption-failures {
        threshold value;
    }
    idp;
    ike-phase1-failures {
        threshold value;
    }
    ike-phase2-failures {
        threshold value;
    }
    key-generation-self-test;
    non-cryptographic-self-test;
    policy {
        application {
            duration interval;
            size count;
            threshold value;
        }
        destination-ip {
            duration interval;
            size count;
            threshold value;
        }
        policy match {
            duration interval;
            size count;
            threshold value;
        }
        source-ip {
            duration interval;
            size count;
            threshold value;
        }
    }
```

```
    replay-attacks {
        threshold value;
    }
    security-log-percent-full percentage;
}
```

Hierarchy Level

```
[edit security alarms]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for potential violation.

Options

authentication—Raise a security alarm when the device or switch detects a specified number of authentication failures (bad password attempts) before an alarm is raised.

cryptographic-self-test—Raise a security alarm when the device or switch detects a cryptographic self-test failure. Cryptographic self-tests are a set of preoperational tests that are performed after the device or switch is powered on. The self-tests run without operator intervention. No alarm is raised upon failure of a cryptographic self-test.

decryption-failures—Raise a security alarm after exceeding a specified number of decryption failures.

encryption-failures—Raise a security alarm after exceeding a specified number of encryption failures.

ike-phase1-failures—Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) Phase 1 failures.

ike-phase2-failures—Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) phase 2 failures.

key-generation-self-test—Raise a security alarm when the device or switch detects a key generation self-test failure. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt data. The self-tests run without operator intervention. No alarm is raised upon failure of a key generation self-test.

non-cryptographic-self-test—Raise a security alarm when the device or switch detects a noncryptographic self-test failure. The self-tests run without operator intervention. No alarm is raised upon failure of a noncryptographic self-test.

non-cryptographic-self-test—Raise a security alarm when the device or switch detects a noncryptographic self-test failure. The self-tests run without operator intervention. No alarm is raised upon failure of a noncryptographic self-test.

policy—Configure alarms for policy violation, based on source IP, destination IP, application, and policy rule.

replay-attacks—Raise a security alarm when the device detects a replay attack.

security-log-percent-full—Raise a security alarm when security log exceeds a specified percent of total capacity.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

pre-id-default-policy

Syntax

```
pre-id-default-policy {
    then {
        log {
            session-init;
            session-close;
        }
        session-timeout {
            icmp seconds;
            icmp6 seconds;
            ospf seconds;
            others seconds;
            tcp seconds;
            udp seconds;
        }
    }
}
```

Hierarchy Level

```
[edit security policies]
```

Release Information

Statement introduced in Junos OS Release 18.2R1.

Description

During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, the SRX Series device applies the default security policy until a more explicit match has occurred. Configures default policy actions that occur prior to dynamic application identification (AppID).

CAUTION: Configuring **session-init** logging for the **pre-id-default-policy** can generate a large amount of logs. Each session that enters the SRX that initially matches the **pre-id-default-policy** will generate an event. We recommend only using this option for troubleshooting purposes.

Options

then—Specifies the policy action that has to be taken when the packet matches the criteria.

log— Specifies the log details at session close time and session initialization time.

Values:

- session-init—Log at the beginning of a session
- session-close—Log at the closure of a session

> **NOTE:** In recent versions of Junos OS, the factory-default configuration of an SRX includes the **session-close** knob. If not already present, we recommend that customers implement **session-close logging** within their **pre-id-default-policy**. This will ensure security logs are generated by the SRX if a flow is unable to leave the **pre-id-default-policy**. These events are generally a result of JDPI being unable to properly classify traffic, although they may also indicate potential attempts at evading the APPID engine.

session-timeout—When you update a session, the session timeout is configured, which specifies the session timeout details in seconds.

Values: icmp—Timeout value for ICMP sessions (seconds)

Range: 4 through 86,400

Values: icmp6—Timeout value for ICMP6 sessions (seconds)

Range: 4 through 86,400

Values: ospf—Timeout value for OSPF sessions (seconds)

Range: 4 through 86,400

Values: others—Timeout value for other sessions (seconds)

Range: 4 through 86,400

Values: tcp—Timeout value for TCP sessions (seconds)

Range: 4 through 86,400

Values: udp—Timeout value for UDP sessions (seconds)

Range: 4 through 86,400

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Advanced Policy-Based Routing

profile(dynamic-application)

Syntax

```
profile name {
    redirect-message {
        type {
            custom-text {
                content content;
            }
            redirect-url {
                content content;
            }
        }
    }
}
```

Hierarchy Level

```
[edit security dynamic-application]
```

Release Information
Statement introduced in Junos OS Release 18.2R1.

Description
Define a profile to provide an explanation for the policy action or to redirect the client request to an informative webpage when a policy blocks HTTP or HTTPS traffic with a deny or reject action in a security policy.

Although drop and reject actions can be logged, the users might not be notified when either action is taken. To provide a reason for the action or to redirect the users to an informative webpage, use the **redirect-message** option at the **[edit security dynamic-application profile** *name***]** hierarchy level to display a custom message.

Customize the redirect action by adding your text message on the splash screen or specify the URL to which the user is redirected. When the **redirect message** option is specified, a splash screen and message informs the client that the traffic has been blocked.

Starting in Junos OS Release 18.2R1, a redirect profile can be configured in a unified policy.

Options
name—Name of the profile.

Values:

redirect-message—Defines the profile of the notification sent to clients when HTTP or HTTPS traffic is blocked by a reject or deny action from an application firewall.

type—The message type displayed after a reject or deny action.

custom-text —Text message in HTML added to the default text. If custom-text is specified, the splash screen displays both the default block message and the custom-defined block message.

The user is redirected when a reject or deny action is taken during one of the following HTTP methods: GET, POST, OPTIONS, HEAD, PUT, DELETE, TRACE, CONNECT, PROPFIND, PROPPATCH, LOCK, UNLOCK, COPY, MOVE, MKCOL, BCOPY, BDELETE, BCOPY, BMOVE, BPROPFIND, BPROPPATCH, POLL, SEARCH, SUBSCRIBE, and UNSUBSCRIBE. If the reject or deny action occurs during a different HTTP method, the traffic is silently dropped.

content—Custom text added to the splash screen. Custom text is inserted below the default message. Add the characters **\n** to insert a line break in the displayed text.

redirect-url —Custom URL redirection.

content—The URL of the webpage to which the client is directed. When traffic is rejected or denied, the client is redirected to the specified webpage for further action. The URL can be hosted on either the SRX Series device or an external server.

Enter the redirect URL in quotation marks for an HTTP or HTTPS site, as shown in the following example:

“https://custom-redirect-url”

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configure a Unified Policy Using a Redirect Message Profile | **154**

dynamic-application (Security) | **326**

protocol (Applications)

Syntax

```
protocol number;
```

Hierarchy Level

```
[edit applications application application-name ]
[edit applications application application-name term term-name]
```

Release Information
Statement modified in Junos OS Release 8.5.

Description
Specify the networking protocol name or number.

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

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

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

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

protocols (Security Zones Host Inbound Traffic)

Syntax

```
protocols {
    (protocol-name | all <protocol-name except>);
}
```

Hierarchy Level

```
[edit security zones security-zone zone-name host-inbound-traffic]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the types of protocol traffic that can reach the device for all interfaces in a zone. You can do this in one of several ways:

- You can enable traffic from each protocol individually.
- You can enable traffic from all protocols.
- You can enable traffic from all but some protocols.

Options

protocol-name—Protocol for which traffic is allowed. The following protocols are supported:

- **all**—Enable traffic from all possible protocols available. Use the *except* option to disallow specific protocols.
- **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.
- **ospf3**—Enable incoming OSPF version 3 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.
- **ripng**—Enable incoming RIP next generation 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) Disable specific incoming protocol traffic, but only when the *all* option has been defined . For example, to enable all but BGP and VRRP protocol traffic:

```
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust host-inbound-traffic protocols bgp except
set security zones security-zone trust host-inbound-traffic protocols vrrp except
```

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

RELATED DOCUMENTATION

Security Zones Overview | **27**

Understanding Functional Zones

protocols (Security Zones Interfaces)

Syntax

```
protocols protocol-name {
    except;
}
```

Hierarchy Level

```
[edit security zones security-zone zone-name interfaces interface-name host-inbound-traffic]
```

Release Information

Statement introduced in Junos OS Release 8.5.

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.
  - **ospf3**—Enable incoming OSPF version 3 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.
  - **ripng**—Enable incoming RIP next generation traffic.
  - **router-discovery**—Enable incoming router discovery traffic.

- **rsvp**—Enable incoming Resource Resolution Protocol (RSVP) traffic (IP protocol number 46).
- **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**.
- **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

except—(Optional) except can only be used if all has been defined.

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

RELATED DOCUMENTATION

Security Zones Overview | 27

Understanding Functional Zones

range-address

Syntax

```
range-address lower-limit to upper-limit;
```

Hierarchy Level

```
[edit security address-book address address-name]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Configure the address range for an address book.

Options

- **lower-limit**—Lower limit of an address range.
- **upper-limit**—Upper limit of an address range.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Address Books | 44

Understanding Address Sets | 47

redirect-wx (Application Services)

Syntax

```
redirect-wx;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
ForSRX300, SRX320, SRX340, SRX345, SRX380, or SRX550M devices, 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.

Specify the WX redirection needed for the packets that arrive from the LAN. Use the **reverse-redirect-wx** statement to specify the WX redirection needed for the reverse flow of the packets that arrive from the WAN.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

reject (Security)

Syntax

```
reject {
    profile redirect-profile-name;
    ssl-proxy {
        profile-name ssl-proxy-profile-name;
    }
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then]
```

Release Information

Statement introduced in Junos OS Release 8.5. Starting in Junos OS Release 19.2, options *profile* and *ssl-proxy* are added.

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**.

You can configure reject action with one of the following options for the dynamic-applications:

- profile - You can chose to provide a notification to the clients or redirect client request to an informative Web page when a policy blocks HTTP or HTTPS traffic with a deny or reject action. To apply a profile, you must define the redirect profile for the dynamic applications.
- ssl-proxy - You can apply a redirect SSL proxy profile when a policy blocks HTTPS traffic with a reject action. When you apply am SSL proxy profile, SSL proxy decrypts the traffic and application identification functionality identifies the application. Next, you can take action to redirect or drop the traffic as per the configuration.

Options

profile—Profile for redirect HTTP/HTTPS traffic.

SSL-proxy—SSL proxy profile for decrypt HTTPS traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

report-skip

Syntax

```
report-skip
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name],
[edit security policies global policy policy-name],
[edit logical-systems logical-system-name security policies from-zone zone-name to-zone zone-name policy policy-name],
[edit logical-systems logical-system-name security policies global policy policy-name],
[edit tenants tenant-name security policies from-zone zone-name policy policy-name],
[edit tenants tenant-name security policies global policy policy-name],
```

Release Information

Statement introduced in Junos OS Release 20.1R1.

Description

You can configure this command to skip policy reports for a policy.

Adding the policy to the policy whitelist excludes the policy from any policy analysis and excluded it from appearing in any future report.

Required Privilege Level

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

RELATED DOCUMENTATION

show security policy-report | 559

reverse-tcp-mss

Syntax

```
reverse-tcp-mss mss-value;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit tcp-options]
```

Release Information
Statement introduced in Junos OS Release 12.3X48-D20.

Description
Configure the TCP maximum segment size (MSS) for packets that match a specific policy and travel in the reverse direction of a session. The value you configure replaces the TCP MSS value when the value in the packet is higher than the one you specify.

The **reverse-tcp-mss** value per policy takes precedence over a global **tcp-mss** value (**all-tcp**, **ipsec-vpn**, **gre-in**, **gre-out**), if one is configured. However, when the **syn-flood-protection-mode syn-proxy** statement at the **[edit security flow] hierarchy level** is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overridden.

Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure the TCP MSS value for the initial session, use the **initial-tcp-mss** option.

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

RELATED DOCUMENTATION

initial-tcp-mss | 353

tcp-mss (Security Flow)

syn-flood-protection-mode

rpc-program-number (Applications)

Syntax

```
rpc-program-number number;
```

Hierarchy Level

```
[edit applications application application-name ]
[edit applications application application-name term term-name]
```

Release Information

Statement modified in Junos OS Release 8.5.

Description

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

Options

number—RPC or DCE program value.

Range: 0 through 65,535

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

scheduler (Security Policies)

Syntax

```
scheduler scheduler-name {
    daily {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    description text;
    friday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    monday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    saturday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    start-date date-time stop-date date-time;
    sunday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    thursday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    tuesday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
    wednesday {
        (all-day | exclude | start-time hh:mm stop-time hh:mm);
    }
}
```

Hierarchy Level

```
[edit schedulers]
[edit tenants <tenant-name> schedulers]
```

Release Information

Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1. The **scheduler** option added under the **set tenants tenant-name schedulers** hierarchy in Junos OS Release 18.3R1.

Description

Create or modify a scheduler that defines when security policies are in effect.

You configure a scheduler to start at a specific date and time or start on a recurrent basis.

Options

scheduler-name —Name of the scheduler. The scheduler 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. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

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 Junos OS Release 8.5.

Description

Specify the schedule (as defined by the **scheduler** ***scheduler-name*** statement) for which the policy is in effect.

Options

scheduler-name —Name of the scheduler.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

schedulers (Security Policies)

Syntax

```
schedulers { ... }
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced in Junos OS Release 8.5. The **schedulers** option added under the **tenants** hierarchy in Junos OS Release 18.3R1.

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. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

screen (Security 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 Junos OS Release 8.5.

Description

Specify a security screen for a security zone.

Options

screen-name —Name of the screen.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Attack Detection and Prevention Overview*
- *Example: Configuring Multiple Screening Options*

secure-domains

Syntax

```
secure-domains [domain-name];
```

Hierarchy Level

```
[edit system services dns dnssec]
```

Release Information
Statement introduced in Junos OS Release 10.2.

Description
Configure secure domains in the DNS server. The server accepts only signed responses for this domain. For unsigned responses, the server returns SERVFAIL error to the client.

Options
domain-name—Name of the domain.

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

RELATED DOCUMENTATION

DNS Overview

secure-neighbor-discovery

Syntax

```
secure-neighbor-discovery {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Provide support for protecting Secure Neighbor Discovery Protocol (SEND) messages.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the Secure Neighbor Discovery (SEND) protocol process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

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

RELATED DOCUMENTATION

security-zone

Syntax

```
security-zone zone-name {
    address-book {
        address address-name {
            ip-prefix {
                description text;
            }
            description text;
            dns-name domain-name {
                ipv4-only;
                ipv6-only;
            }
            range-address lower-limit to upper-limit;
            wildcard-address ipv4-address/wildcard-mask;
        }
        address-set address-set-name {
            address address-name;
            address-set address-set-name;
            description text;
        }
    }
    advance-policy-based-routing;
    application-tracking;
    description text;
    enable-reverse-reroute;
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
```

```
    }
  }
  screen screen-name;
  tcp-rst;
}
```

Hierarchy Level

```
[edit security zones]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

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. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Zones Overview | 27

Example: Configuring Application Firewall Rule Sets Within a Security Policy

sequence-check-required

Syntax

```
sequence-check-required;
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tcp-options]

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Enable sequence check per policy. The sequence-check-required value overrides the global value no-sequence-check.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | 23
- Understanding Security Policy Rules | 106
- Understanding Security Policy Elements | 105

services-offload (Security)

Syntax

```
services-offload;
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Enable services offloading within a security policy for SRX4600, SRX5400, SRX5600, and SRX5800 devices.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Elements | 105

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 Junos OS Release 8.5.

Description

Enable traffic to which the policy applies to be logged at the end of a session.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | **23**
- Understanding Security Policy Rules | **106**
- Understanding Security Policy Elements | **105**

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 Junos OS Release 8.5.

Description

Enable traffic to which the policy applies to be logged at the beginning of a session.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | **23**
- Understanding Security Policy Rules | **106**
- Understanding Security Policy Elements | **105**

simple-mail-client-service

Syntax

```
simple-mail-client-service {
    command binary-file-path;
    disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the SMTP client process.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the SMTP client process.

Required Privilege Level

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

RELATED DOCUMENTATION

source-address (Security Policies)

Syntax

```
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information

Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.

Description

Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

Options

address—IP addresses, address sets, or wildcard addresses (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Rules | 106

Understanding Security Policy Elements | 105

source-address-excluded

Syntax

```
source-address-excluded;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name match]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

Description

Exclude the source address(es) from the policy.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

source-identity

Syntax

```
source-identity {
    [user-or-role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

[edit security advance-policy-based-routing from-zone *zone-name* policy *policy-name* match]

Release Information

Statement introduced in Junos OS Release 12.1. Statement updated in Junos OS Release 12.1X44-D10. Statement is supported in [edit security advance-policy-based-routing from-zone *zone-name* policy *policy-name* match] hierarchy in Junos OS Release 19.1R1.

Description

Identifies users and roles to be used as match criteria for a policy. If a value other than **any** is specified as match criteria for a policy within a zone pair, the traffic is matched to table entries to retrieve associated user and roles before policy lookup occurs. Users and roles are retrieved from the local authentication table or from a UIT pushed to the SRX Series device from an access control service when a user is authenticated.

Options

The following entries specify the source identities that match a policy:

user-or-role-name—A list of specific users and roles.

Range: 0 through 39 characters

NOTE: SRX Series devices truncate imported roles to 39 characters. You need to ensure that all of your roles are 39 characters or less.

any—Any user or role, as well as the keywords authenticated-user, unauthenticated-user, and unknown-user.

authenticated-user—All users and roles that have been authenticated.

unauthenticated-user—Any user or role that does not have an IP-address mapped to authentication sources and the authentication source is up and running.

unknown-user—Any user or role that does not have an IP address mapped to authentication sources, because the authentication source is disconnected from the SRX Series device. In this case, users are unable to be authenticated due to an authentication server disconnection, such as a power outage.

Unknown-user must be configured for non-domain users to be able to authenticate and log in.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding User Role Firewalls | **183**
- Understanding the User Identification Table | **186**
- Security Policies Overview | **23**

source-ip (Security Alarms)

Syntax

```
source-ip {
    duration interval;
    size count;
    threshold value;
}
```

Hierarchy Level

```
[edit security alarms potential-violation policy]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure alarms for a number of policy violations by a source network identifier within a specified time period.

Options

- **duration *interval***—Indicate the duration of counters.

Range: 1 through 3600 seconds.

Default: 1 second.

- **size *count***—Indicate the number of source IP addresses for which policy violation checks can be done concurrently.

Range: 1 through 10240.

Default: 1024.

- **threshold *value***—Indicate the maximum number of source IP address matches required to raise an alarm.

Range: 1 through 4294967295.

Default: 1000.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

source-port (Applications)

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 Junos OS Release 8.5.

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 **destination-port (Applications)**.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Application Sets Overview | 70

ssl-proxy (Application Services)

Syntax

```
ssl-proxy {
    profile-name profile-name
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Enable SSL proxy and identify the name of the SSL proxy profile to be used. This option is supported on SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

Options

profile-name—SSL proxy profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SSL Forward Proxy

ssl-termination-profile

Syntax

```
ssl-termination-profile profile-name;
```

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 Junos OS Release 12.1X44-D10.

Description

Specify the SSL termination profile used for SSL offloading.

Options

profile-name—Specify the name of the SSL termination profile used to the SSL offload.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

start-date

Syntax

```
start-date date-time;
```

Hierarchy Level

```
[edit schedulers scheduler scheduler-name]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Specify the time, day, month, and year that the schedule starts.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

Options
date-time —Use the format **[*yyyy* -] *mm* - *dd* . *hh* . *mm*** to specify the year, month, day, hour, and minutes.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

start-time (Schedulers)

Syntax

```
start-time hh:mm;
```

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 Junos OS Release 8.5.

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 **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the starting time specified for a specific day (for example, Friday using the **friday** statement) overrides the starting time set with the **daily** statement.

Options

time —Use the 24-hour format (***hh:mm:ss***) to specify the hours, minutes, and seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

stop-date

Syntax

```
stop-date date-time;
```

Hierarchy Level

```
[edit schedulers scheduler scheduler-name]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Specify the time, day, month, and year that the schedule ends.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

Options
date-time —Use the format **[** ***yyyy*** **-]** ***mm*** **-** ***dd*** **.** ***hh*** **.** ***mm*** to specify the year, month, day, hour, and minutes.

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

RELATED DOCUMENTATION

Security Policies Overview | 23

stop-time

Syntax

```
stop-time hh:mm;
```

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 Junos OS Release.

Description

Specify the time that a schedule stops for a specified day.

If you specify a stop time for a daily schedule with the **daily** statement and also include the the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the stop time specified for a specific day (for example, Friday using the **friday** statement) overrides the stop time set with the **daily** statement.

Options

time —Use the 24-hour format (***hh:mm:ss***) to specify the hours, minutes, and seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

syn-check-required

Syntax

```
syn-check-required;
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit tcp-options]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.

Required Privilege Level

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

RELATED DOCUMENTATION

Attack Detection and Prevention Overview

Example: Configuring Multiple Screening Options

system-services (Security Zones Host Inbound Traffic)

Syntax

```
system-services {
    (service-name | all <service-name except>);
}
```

Hierarchy Level

```
[edit security zones security-zone zone-name host-inbound-traffic]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the types of incoming system service traffic that can reach the device for all interfaces in a zone. You can do this in one of several ways:

- You can enable traffic from each system service individually.
- You can enable traffic from all system services.
- You can enable traffic from all but some system services.

Options

- ***service-name*** —System-service for which traffic is allowed. The following system services are supported:
  - **all**—Enable traffic from the defined system services available on the Routing Engine (RE). Use the *except* option to disallow specific system services. Enabling all the system services does not override any interface specific configuration under a particular zone.
  - **any-service**—Enable all system services on entire port range including the system services that are not defined.
  - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
  - **dhcp**—Enable incoming DHCP requests.
  - **dhcpv6**—Enable incoming DHCP requests for IPv6.
  - **dns**—Enable incoming DNS services.
  - **finger**—Enable incoming finger traffic.
  - **ftp**—Enable incoming FTP traffic.
  - **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).
- **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
- **ike**—Enable Internet Key Exchange traffic.
- **lsping**—Enable label switched path ping service.
- **netconf**—Enable incoming NETCONF service.
- **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
- **ping**—Allow the device to respond to ICMP echo requests.
- **r2cp**—Enable incoming Radio Router Control Protocol traffic.
- **reverse-ssh**—Reverse SSH traffic.
- **reverse-telnet**—Reverse Telnet traffic.
- **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-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

- **except**—(Optional) Enable specific incoming system service traffic but only when the *all* option has been defined . For example, to enable all but FTP and HTTP system service traffic:

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic system-services ftp except
set security zones security-zone trust host-inbound-traffic system-services http except
```

Required Privilege Level

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

RELATED DOCUMENTATION

Security Zones Overview | 27

Supported System Services for Host Inbound Traffic | 32

system-services (Security Zones Interfaces)

Syntax

```
system-services service-name {
    except;
}
```

Hierarchy Level

```
[edit security zones security-zone zone-name interfaces interface-name host-inbound-traffic]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the types of traffic that can reach the device on a particular interface.

Options

- ***service-name*** —Service for which traffic is allowed. The following services are supported:
  - **all**—Enable all possible system services available on the Routing Engine (RE).
  - **any-service**—Enable services on entire port range.
  - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
  - **dhcp**—Enable incoming DHCP requests.
  - **dhcpv6**—Enable incoming DHCP requests for IPv6.
  - **dns**—Enable incoming DNS services.
  - **finger**—Enable incoming finger traffic.
  - **ftp**—Enable incoming FTP traffic.
  - **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).
  - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
  - **ike**—Enable Internet Key Exchange traffic.
  - **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
  - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
  - **ping**—Allow the device to respond to ICMP echo requests.

- **r2cp**—Enable incoming Radio Router Control Protocol traffic.
- **reverse-ssh**—Reverse SSH traffic.
- **reverse-telnet**—Reverse Telnet traffic.
- **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-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

- **except**—(Optional) except can only be used if all has been defined.

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

RELATED DOCUMENTATION

Security Zones Overview | 27

Supported System Services for Host Inbound Traffic | 32

tcp-options (Security Policies)

Syntax

```
tcp-options {
    initial-tcp-mss mss-value;
    reverse-tcp-mss mss-value;
    sequence-check-required;
    syn-check-required;
    window-scale;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* security **policies from-zone**],
[edit logical-systems *logical-system-name* security **policies global** policy *name* then],
[edit logical-systems *logical-system-name* security **policies** stateful-firewall-rule *name* policy *name* then],
[edit logical-systems *logical-system-name* tenants *name* security **policies from-zone**],
[edit logical-systems *logical-system-name* tenants *name* security **policies global** policy *name* then],
[edit logical-systems *logical-system-name* tenants *name* security **policies** stateful-firewall-rule *name* policy *name* then],
[edit security **policies**]
[edit security **policies global** policy *name* then],
[edit security **policies** stateful-firewall-rule *name* policy *name* then],
[edit tenants *tenant-name* security **policies from-zone**],
[edit tenants *tenant-name* security **policies global** policy *name* then],
[edit tenants *tenant-name* security **policies** stateful-firewall-rule *name* policy *name* then]
[edit security **policies from-zone** *zone-name* **to-zone** *zone-name* **policy** *policy-name* **then permit**]

Release Information

The **tcp-options**, **sequence-check-required**, and **syn-check-required** statements are introduced in Junos OS Release 10.4.
The **initial-tcp-mss** and **reverse-tcp-mss** statements are introduced in Junos OS Release 12.3X48-D20.
The **window-scale** statement is introduced in Junos OS Release 15.1X49-D70.

Description

Specify the TCP options for each policy. You can configure sync and sequence checks for each policy based on your requirements, and, because each policy has two directions, you can configure a TCP MSS value for both directions or for just one direction. To configure per-policy TCP options, you must turn off the respective global options. Otherwise, the commit check will fail.

Options

initial-tcp-mss—Configure the TCP maximum segment size (MSS) for packets that arrive at the ingress interface (initial direction), match a specific policy, and for which a session is created. The value you configure overrides the TCP MSS value in the incoming packet when the value in the packet is higher than the one you specify.

The **initial-tcp-mss** value per policy takes precedence over a global **tcp-mss** value (**all-tcp**, **ipsec-vpn**, **gre-in**, **gre-out**), if one is configured. However, when the **syn-flood-protection-mode syn-proxy** statement at the **[edit security flow]** hierarchy level is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overriden.

Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure a TCP MSS value for the reverse session, use the **reverse-tcp-mss** option.

Range: 64 through 65535

reverse-tcp-mss—Configure the TCP maximum segment size (MSS) for packets that match a specific policy and travel in the reverse direction of a session. The value you configure replaces the TCP MSS value when the value in the packet is higher than the one you specify.

The **reverse-tcp-mss** value per policy takes precedence over a global **tcp-mss** value (**all-tcp**, **ipsec-vpn**, **gre-in**, **gre-out**), if one is configured. However, when the **syn-flood-protection-mode syn-proxy** statement at the **[edit security flow]** hierarchy level is used to enable SYN proxy defenses against SYN attacks, the TCP MSS value is not overridden.

Because each policy has two directions, you can configure a value for both directions or for just one direction. To configure the TCP MSS value for the initial session, use the **initial-tcp-mss** option.

Range: 64 through 65535

sequence-check-required—Enable sequence check per policy. The sequence-check-required value overrides the global value no-sequence-check.

syn-check-required—Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.

window-scale—Enable window-scale per policy.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Rules | 106

Understanding Security Policy Elements | 105

tcp-rst

Syntax

```
tcp-rst;
```

Hierarchy Level

```
[edit security zones security-zone zone-name]
```

Release Information
Statement introduced in Junos OS Release 8.5.

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.

During flow first path process, a TCP RST packet is sent to the traffic originator if the TCP packet trying to create the flow session is not a SYN packet.

Default
By default, **tcp-rst** is disabled.

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

RELATED DOCUMENTATION

Example: Configuring the TCP-Reset Parameter | 40

term (Applications)

Syntax

```
term term-name {
    alg application;
    destination-port port-identifier;
    icmp-code value;
    icmp-type value;
    icmp6-code value;
    icmp6-type value;
    inactivity-timeout (seconds | never);
    protocol number;
    rpc-program-number number;
    source-port port-number;
    uuid hex-value;
}
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Define individual application protocols.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policy Applications Overview | 69

then (Security Policies)

Syntax

```
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
                profile-name profile-name;
            }
            uac-policy {
                captive-portal captive-portal;
            }
            utm-policy policy-name;
        }
        destination-address {
            drop-translated;
            drop-untranslated;
        }
        firewall-authentication {
            pass-through {
                access-profile profile-name;
                client-match user-or-group-name;
```

```
            ssl-termination-profile profile-name;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile profile-name;
            domain domain-name
            ssl-termination-profile profile-name;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        initial-tcp-mss mss-value;
        reverse-tcp-mss mss-value;
        sequence-check-required;
        syn-check-required;
    }
    tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
        pair-policy pair-policy;
    }
  }
  reject;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.

Description

Specify the policy action to be performed when packets match the defined criteria.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | 23
- Understanding Security Policy Rules | 106
- Understanding Security Policy Elements | 105

to-zone (Security Policies)

Syntax

```
to-zone zone-name {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
            destination-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-identity {
                [role-name];
                any;
                authenticated-user;
                unauthenticated-user;
                unknown-user;
            }
        }
        scheduler-name scheduler-name;
        then {
            count {
                alarm {
                    per-minute-threshold number;
                    per-second-threshold number;
                }
            }
            deny;
            log {
                session-close;
                session-init;
```

```
}
```

```
permit {
    application-services {
        application-firewall {
            rule-set rule-set-name;
        }
        application-traffic-control {
            rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
        uac-policy {
            captive-portal captive-portal;
        }
        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            ssl-termination-profile profile-name;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        sequence-check-required;
        syn-check-required;
    }
    tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
```

```
                pair-policy pair-policy;
            }
        }
        reject;
    }
  }
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** and **junos-host** options added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

Description

Specify a destination zone to be associated with the security policy.

Options

- **zone-name**—Name of the destination zone object.
- **junos-host**—Default security zone for self-traffic of the device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Rules | 106

Understanding Security Policy Elements | 105

to-zone (Security Policies Global)

Syntax

```
to-zone {
    [zone-name];
    any;
}
```

Hierarchy Level

```
[edit security policies global policy policy-name match]
```

Release Information

Statement introduced in Junos OS Release 12.1X47-D10.

Description

Identify a single destination zone or multiple destination zones to be used as a match criteria for a policy. You must configure specific zones or default to any zone, but you cannot have both in a global policy.

Required Privilege Level

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

RELATED DOCUMENTATION

- Global Policy Overview | 172
- Example: Configuring a Global Policy with No Zone Restrictions | 175
- Example: Configuring a Global Policy with Multiple Zones | 179

traceoptions (dynamic-application)

Syntax

```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

```
[edit security dynamic-application]
[edit security dynamic-address]
```

Release Information

Statement introduced in Junos OS Release 18.2R1.

Description

Configure dynamic application tracing options.

> **NOTE:** NOTE: Traceoptions does not differentiate between a logical system and tenant system, and can be configured under the root logical system.

Options

file—Trace file information

Values:

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**. By default, the name of the file is the name of the process being traced.

files *number*—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed as ***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

Default: 3 files

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

size *maximum-file-size*—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.

Range: 10 KB through 1 GB

Default: 128 KB

world-readable|no-world-readable—By default, the 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—Configure tracing parameters

Values:

all—Trace with all flags enabled.

configuration—Trace configuration events.

compilation—Trace compilation events.

ipc—Trace process intercommunication events.

lookup—Trace lookup 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.

RELATED DOCUMENTATION

Unified Policies Overview | **145**

Unified Policies Configuration Overview | **146**

traceoptions (Security Policies)

Syntax

```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

[edit security policies]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Configure policy tracing options.

Options

- **file**—Configure the trace file options.
  - ***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**. By default, the name of the file is the name of the process being traced.
  - **files *number***—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***—Refine the output to include lines that contain the regular expression.

- **size *maximum-file-size***—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 a 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**—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
- **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.

RELATED DOCUMENTATION

Security Policies Overview | 23

traceoptions (Security User Identification)

Syntax

```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

```
[edit security user-identification]
```

Release Information
Statement introduced in Junos OS Release 12.1.

Description
Configure flow tracing options.

Options

- **file**—Configure the trace file options.
  - *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**. By default, the name of the file is the name of the process being traced.
  - **files** *number*—Maximum number of trace files. When a trace file named ***trace-file*** 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***—Refine the output to include lines that contain the regular expression.

- **size *maximum-file-size***—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 a 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**—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.
  - **all**—Trace with all flags enabled
  - **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.

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

traceoptions (System Services DNS)

Syntax

```
traceoptions {
    category {
        category-type;
    }
    file;
}
```

Hierarchy Level

```
[edit system services dns]
```

Release Information

Statement introduced in Junos OS Release 10.2.

Description

Defines tracing options for DNS services.

Options

category—Specifies the logging category. See Table 34 on page 462 for the different logging categories and their descriptions.

file—Trace file information.

Table 34: Category Names

Category Name	Description
client	Processing of client requests
config	Configuration file parsing and processing
database	Messages relating to the databases
default	Categories for which there is no specific configuration
delegation-only	Delegation only
dispatch	Dispatching of incoming packets to the server
dnssec	DNSSEC and TSIG protocol processing
edns-disabled	Log query using plain DNS
general	General information
lame-servers	Lame servers
network	Network options
notify	NOTIFY protocol
queries	DNS query resolver
resolver	DNS resolution security
security	Approval and denial of requests
unmatched	Unable to determine the class for messages named
update	Dynamic updates
update-security	Approval and denial of update requests
xfer-in	Zone transfers that the server is receiving xfer-out
xfer-out	Zone transfers that the server is sending

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- *DNS Overview*

tunnel (Security Policies)

Syntax

```
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit]
```

Release Information

Statement introduced in Junos OS Release 8.5. The **ipsec-group-vpn** option added in Junos OS Release 10.2.

Description

Encapsulate outgoing IP packets and decapsulate incoming IP packets.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Security Policies Overview | 23
- Understanding Security Policy Rules | 106
- Understanding Security Policy Elements | 105

uac-policy (Application Services)

Syntax

```
uac-policy {
    captive-portal captive-portal;
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services]
```

Release Information

Statement modified in Junos OS Release 9.4.

Description

Enable Unified Access Control (UAC) for the security policy. This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series UAC Appliance .

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

Example: Configuring a User Role Firewall on an SRX Series Device | 195

unified-access-control (Security)

Syntax

```
unified-access-control priority priority;
```

Hierarchy Level

```
[edit security user-identification authentication-source]
```

Release Information

Statement introduced in Junos OS Release 12.1. Support for **disable** option dropped in Junos OS Release 12.1X47-D10.

Description

An authentication table pushed from a configured authentication device, such as the Junos Pulse Access Control Service.

Options

priority *priority*—A unique value between 0 and 65535 that determines the sequence for searching multiple tables to retrieve a user role. Each authentication table is given a unique priority value. The lower the value, the higher the priority. A table with priority 120 is searched before a table with priority 200. The default priority value of the unified-access-control authentication table is 200.

Setting the priority value of the unified-access-control authentication table to 0 is equivalent to disabling the table and eliminating it from the search sequence.

Required Privilege Level

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

RELATED DOCUMENTATION

- authentication-source (Security) | 304
- Understanding User Role Firewalls | 183
- Understanding the User Identification Table | 186

unified-policy-explicit-match

Syntax

```
unified-policy-explicit-match;
```

Hierarchy Level

[edit security policies]

Release Information

Statement introduced in Junos OS Release 18.2R1.

Description

Enable explicit match in a unified policy.

- In a unified policy, when you enable explicit match, the session is dropped if a dependent application does not have any matching policy.
- In a unified policy, when explicit match is not configured, then implicit match is applied. That is, if the dependent application does not have a matching policy, then the security policy that is configured for the base application is applied.

By default, the unified policies enforce implicit rules on dependent applications.

Required Privilege Level

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

RELATED DOCUMENTATION

Unified Policies Configuration Overview | 146
Unified Policies Overview | 145

user-firewall

Syntax

```
user-firewall {
    access-profile profile-name;
    domain domain-name
    ssl-termination-profile profile-name;
}
```

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 Junos OS Release 12.1X45-D10. Support for the **domain** keyword added in Junos OS Release 12.1X47-D10.

Description

Configure user role firewall authentication, and map the source IP address to the username and its associated roles (groups). The mapped data is written to the firewall authentication table for later retrieval by the user role firewall. The user role firewall uses the username and role information to determine whether to permit or deny a user's session or traffic.

Options

access-profile *profile-name*—Specify the name of the access profile to be used for authentication.

domain *domain-name*—Specify the name of the domain where firewall authentication occurs in the event that the Windows Management Instrumentation client (WMIC) is not available to get IP-to-user mapping for the integrated user firewall feature. The maximum length is 65 bytes.

ssl-termination-profile *profile-name*—For HTTPS traffic, specify the name of the SSL termination profile used for SSL offloading.

Required Privilege Level

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

RELATED DOCUMENTATION

Overview of Integrated User Firewall

Using Firewall Authentication as an Alternative to WMIC

Understanding User Role Firewalls | **183**

Example: Configuring a User Role Firewall on an SRX Series Device | **195**

user-identification

Syntax

```
user-identification {
    authentication-source {
        firewall-authentication (disable | priority priority);
        local-authentication-table (disable | priority priority);
        unified-access-control (disable | priority priority);
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 12.1. Statement updated in Junos OS Release 12.1X45-D10.

Description

Identifies one or more tables to be used as the source for user role information.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

Understanding the User Identification Table | 186

utm-policy

Syntax

```
utm-policy policy-name {
    anti-spam {
        smtp-profile profile-name;
    }
    anti-virus {
        ftp {
            download-profile profile-name;
            upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
    }
    content-filtering {
        ftp {
            download-profile profile-name;
            upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
    }
    traffic-options {
        sessions-per-client {
            limit value;
            over-limit (block | log-and-permit);
        }
    }
    web-filtering {
        http-profile profile-name;
    }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm]
```

Release Information

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure a UTM policy for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols and attach this policy to a security profile to implement it.

Options

policy-name—Specify name of the UTM policy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Security Policies Overview | **23**
- Understanding Security Policy Rules | **106**
- Understanding Security Policy Elements | **105**

uuid (Applications)

Syntax

```
uuid hex-value;
```

Hierarchy Level

```
[edit applications application application-name  term  term-name]
```

Release Information
Statement modified in Junos OS Release 8.5.

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

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

Options
uuid *hex-value* —Specify the universal unique identifier (UUID) for objects.

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

RELATED DOCUMENTATION

vrrp

Syntax

```
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the Virtual Router Redundancy Protocol (VRRP) process.

Options

- **command *binary-file-path***—Path to the binary process.
- **disable**—Disable the VRRP process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

> **NOTE:** On SRX300 and SRX320 devices, you cannot configure the same VRRP group ID on different interfaces of a single device

Required Privilege Level

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

RELATED DOCUMENTATION

web-authentication

Syntax

```
web-authentication {
    client-match user-or-group-name;
}
```

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 Junos OS Release 8.5.
HTTPS for Web authentication is supported on SRX5400, SRX5600, and SRX5800 devices starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.

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 or HTTPS request is redirected.

Options

client-match ***user-or-group*** —(Optional) Username or user group name.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

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 user-firewall]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, support for user-firewall added on SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX Services Gateways.

Description

Optionally, redirect HTTP requests to the device's internal webserver by sending a redirect HTTP response to the client system to reconnect to the webserver for user authentication. The interface on which the client's request arrived is the interface to which the request is redirected.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

zones

Syntax

```
zones {
    functional-zone {
        management {
            description text;
            host-inbound-traffic {
                protocols protocol-name {
                    except;
                }
                system-services service-name {
                    except;
                }
            }
            interfaces interface-name  {
                host-inbound-traffic {
                    protocols protocol-name {
                        except;
                    }
                    system-services service-name {
                        except;
                    }
                }
            }
            screen screen-name;
        }
    }
    security-zone zone-name {
        address-book {
            address address-name {
                ip-prefix {
                    description text;
                }
                description text;
                dns-name domain-name {
                    ipv4-only;
                    ipv6-only;
                }
                range-address lower-limit to upper-limit;
                wildcard-address ipv4-address/wildcard-mask;
            }
            address-set address-set-name {
```

```
            address address-name;
            address-set address-set-name;
            description text;
        }
    }
    advance-policy-based-routing;
    application-tracking;
    description text;
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
    tcp-rst;
  }
}
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description

A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Security Zones Overview | 27
Supported System Services for Host Inbound Traffic | 32

CHAPTER 7

Operational Commands

clear security alarms | 483

clear security policies hit-count | 487

clear security policies statistics | 488

clear system services dns dns-proxy | 489

request security policies check | 490

request security policies resync | 493

request security user-identification local-authorization-table add | 495

request security user-identification local-authentication-table delete | 497

show security alarms | 499

show security firewall-authentication users address | 505

show security firewall-authentication users auth-type | 509

show security flow session application | 512

show security match-policies | 517

show security policies | 524

show security policies checksum | 541

show security policies hit-count | 544

show security policies information | 548

show security policies unknown-source-identity | 554

show security policies zone-context | 556

show security policy-report | 559

show security shadow-policies | 563

show security user-identification local-authentication-table | 566

show security user-identification role-provision all | 569

show security user-identification source-identity-provision all | 571

show security user-identification user-provision all | 573

show security zones | 575

show security zones type | 583

show system services dns dns-proxy | 587

show system services dynamic-dns | 590

clear security alarms

Syntax

```
clear security alarms
<all>
<alarm-id id-number>
<alarm-type [ types ]>
<newer-than YYYY-MM-DD.HH:MM:SS>
<older-than YYYY-MM-DD.HH:MM:SS>
<process process>
<severity severity>
```

Release Information

Command introduced in Junos OS Release 11.2.

Description

Clear (acknowledge) the alarms that are active on the device.

Options

all—(Optional) Clear all active alarms.

alarm-id *id-number*—(Optional) Clear the specified alarm.

alarm-type [*types*]—(Optional) Clear the specified alarm type or a set of types.

You can specify one or more of the following alarm types:

- **authentication**
- **cryptographic-self-test**
- **decryption-failures**
- **encryption-failures**
- **ike-phase1-failures**
- **ike-phase2-failures**
- **key-generation-self-test**
- **non-cryptographic-self-test**
- **policy**
- **replay-attacks**

newer-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Clear active alarms that were raised after the specified date and time.

older-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Clear active alarms that were raised before the specified date and time.

process *process*—(Optional) Clear active alarms that were raised by the specified system process.

severity *severity*—(Optional) Clear active alarms of the specified severity.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

Required Privilege Level

security—To view this statement in the configuration.

RELATED DOCUMENTATION

show security alarms | 499

Troubleshooting Security Policies | 269

List of Sample Output

clear security alarms all on page 485
clear security alarms alarm-id <alarm-id> on page 485
clear security alarms alarm-type authentication on page 485
clear security alarms newer-than <time> on page 485
show security alarms older-than <time> on page 485
show security alarms process <process> on page 485
show security alarms severity <severity> on page 486

Output Fields

This command produces no output, except a statement about the number of security alarms cleared.

Sample Output

clear security alarms all

```
[3 SECURITY ALARMS] user@router> clear security alarms all

3 security alarms cleared
```

clear security alarms alarm-id <alarm-id>

```
[3 SECURITY ALARMS] user@router> clear security alarms alarm-id 1

1 security alarm cleared
```

clear security alarms alarm-type authentication

```
[3 SECURITY ALARMS] user@router> clear security alarms alarm-type authentication

3 security alarms cleared
```

clear security alarms newer-than <time>

```
[3 SECURITY ALARMS] user@router> clear security alarms newer-than 2010-01-19.13:41:59

1 security alarm cleared
```

show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> clear security alarms older-than 2010-01-19.13:41:59

2 security alarms cleared
```

show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> clear security alarms process sshd
```

```
3 security alarms cleared
```

show security alarms severity <severity>

`[3 SECURITY ALARMS] user@router>` **clear security alarms severity notice**

```
3 security alarms cleared
```

clear security policies hit-count

Syntax

```
clear security policies hit-count
<from-zone zone-name>
<to-zone zone-name>
```

Release Information

Command introduced in Junos Release 12.1.

Description

Clear the hit-count values for security policies.

Options

- **from-zone *zone-name***—(Optional) Clear the number of hits for security policies associated with the named source zone.
- **to-zone *zone-name***—(Optional) Clear the number of hits for security policies associated with the named destination zone.

Required Privilege Level

clear

RELATED DOCUMENTATION

show security policies hit-count | 544

Monitoring Security Policy Statistics | 266

Output Fields

This command produces no output.

clear security policies statistics

Syntax

```
clear security policies statistics
```

Release Information

Command introduced in Junos OS Release 8.5. Support for systemwide policies statistics added in Junos OS Release 12.1X46-D10.

Description

Clear systemwide policies statistics and security policies statistics configured on the device.

Required Privilege Level

clear

RELATED DOCUMENTATION

show security policies | 524

Monitoring Security Policy Statistics | 266

Output Fields

This command produces no output.

clear system services dns dns-proxy

Syntax

```
clear system services dns dns-proxy
```

Release Information

Command introduced in Junos OS Release 12.1X44-D10.

Description

Clear DNS proxy cache information. This option is supported on the SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices.

Options

- **cache**—Clear DNS proxy cache information.
- **statistics**—Clear DNS proxy statistics.
- **none**—Clear all DNS proxy cache information.
- **hostname**—(Optional) Clear DNS proxy cache information from the specified host.

Required Privilege Level

clear

RELATED DOCUMENTATION

show system services dns dns-proxy | 587

show system services dynamic-dns | 590

Output Fields

When you enter this command no output is produced.

request security policies check

Syntax

```
request security policies check
<from-zone zone name>
<global>
<logical-system (logical-system name | all)>
<pfe>
<root-logical-system>
<to-zone zone-name>
<tenant tenant-name>
```

Release Information

Command introduced in Junos OS Release 18.4R1.

Description

Displays the security policy sync status between the Routing Engine and the Packet Forwarding Engine. Use the command to display a list of all security polices which are in-sync or out-of-sync on the device.

Use the **show security policies checksum** command to display the security policy checksum value and use the **request security policies resync** command to synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine.

Options

<from-zone *zone-name*—Displays security policies sync status from this zone.

global—Displays global policies sync status.

logical-system (*logical-system name* | all)—Displays security policies sync status for the security policies configured on a logical system or on all logical systems.

pfe—Displays security policies sync status for the security policies on the Packet Forwarding Engine.

root-logical-system—Displays security policies sync status for the security policies configured on the root logical system. This is the default outcome.

to-zone *zone-name*—Displays security policies sync status to this zone.

tenant *tenant-name*—Displays security policies sync status for the security policies configured on a tenant.

Additional Information

Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of

a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.
- An error with the routing engine, such as a reused policy UID.

When the policy configurations are modified and the policies are out of sync, the following error message displays - **error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)>. Please request security policies check/resync**.

Required Privilege Level
view

RELATED DOCUMENTATION

request security policies resync | 493
show security policies checksum | 541

List of Sample Output
request security policies check on page 491
request security policies check logical-system LSYS1 on page 491
request security policies check logical-system all on page 492
request security policies check from-zone trust to-zone untrust on page 492

Sample Output

request security policies check

```
user@host> request security policies check
```

```
Start sending policies ...
Success
Total sent 1 policy.

Policy Checking Result:
 PFE master            in-sync
```

request security policies check logical-system LSYS1

```
user@host> request security policies check logical-system LSYS1
```

```
Start sending policies ...
Success
Total sent 1 policy.

Policy Checking Result:
 PFE fpc0.pic3         in-sync
 PFE fpc0.pic1         in-sync
 PFE fpc0.pic0         in-sync
 PFE fpc0.pic2         in-sync
```

request security policies check logical-system all

user@host> **request security policies check logical-system all**

```
Start sending policies ...
Success
Total sent 2 policies.

Policy Checking Result:
 PFE fpc0.pic1         in-sync
 PFE fpc0.pic3         in-sync
 PFE fpc0.pic2         in-sync
 PFE fpc0.pic0         in-sync
```

request security policies check from-zone trust to-zone untrust

user@host> **request security policies check from-zone trust to-zone untrust**

```
Start sending policies ...
Success
Total sent 2 policies.

Policy Checking Result:
 PFE fpc4.pic0         in-sync
 PFE fpc4.pic1         out-of-sync
```

request security policies resync

Syntax

```
request security policies resync
<from-zone zone name>
<global>
<logical-system (logical-system name | all)>
<pfe>
<root-logical-system>
<to-zone zone-name>
<tenant tenant-name>
```

Release Information

Command introduced in Junos OS Release 18.4R1.

Description

Synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine.

This command recovers the security policies in the Packet Forwarding Engine. If policy inconsistencies between the Routing Engine and Packet Forwarding Engine are determined, the security policies resync.

Options

<from-zone *zone-name*—Recover the policies from this zone.

global—Recover global policies.

logical-system (*logical-system name* | all)—Recover the policies on all logical systems or on a particular logical system.

pfe—Recover the policies on the Packet Forwarding Engine.

root-logical-system—Recover the policies on the root logical system. This is the default option.

to-zone *zone-name*—Recover the policies to this zone.

tenant *tenant-name*—Recover the policies of a tenant.

Additional Information

Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.

- An error with the routing engine, such as a reused policy UID.

When the policy configurations are modified and the policies are out of sync, the following error message displays - **error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)>. Please request security policies check/resync**.

Use the **show security policies checksum** command to display the security policy checksum value and use the **request security policies check** to display the security policy sync status.

Required Privilege Level
view

RELATED DOCUMENTATION

request security policies check | 490

show security policies checksum | 541

List of Sample Output
request security policies resync on page 494
request security policies resync logical-system all on page 494

Sample Output

request security policies resync

`user@host>` **request security policies resync**

```
Start sending policies ...
Success
Total sent 1 policy.
```

request security policies resync logical-system all

`user@host>` **request security policies resync logical-system all**

```
Start sending policies ...
Success
Total sent 2 policies.
```

request security user-identification local-authorization-table add

Syntax

```
request security user-identification local-authorization-table add user user-name ip-address ip-address roles [role-name]
```

Release Information

Command introduced in Junos OS Release 12.1. Command updated in Junos OS Release 12.1X44-D10.

Description

This command adds user and role information to the local authentication table. The table is used to retrieve user and role information for traffic from the specified IP address to enforce a user role firewall.

To add an entry, specify the user name, IP address, and up to 40 roles to be associated with this user. Subsequent commands for the same user and IP address aggregates any new roles to the existing list. An authentication entry can contain up to 200 roles.

NOTE: To change the user name of an entry or to remove or change entries in a role list, you must delete the existing entry and create a new one.

An IP address can be associated with only one user. If a second request is made to add a different user using the same IP address, the second authentication entry overwrites the existing entry.

Options

user *user-name*—Specify the name of the user to be added to the table.

ip-address *ip-address*—Specify the IP address of the user. Either IPv4 or IPv6 addresses are supported.

roles [*role-name*]—(Optional) Specify the role or list of roles to be associated with the specified user. If the specified user and IP address already exist, any roles specified in the command are added to the existing role list.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

request security user-identification local-authentication-table delete | 497

Understanding the User Identification Table | 186

List of Sample Output

request security user-identification local-authentication-table add on page 496

Output Fields

When you enter this command, either an entry is added to the local authentication table, or the roles of an existing entry are aggregated with additional roles.

Sample Output

request security user-identification local-authentication-table add

```
user@host> request security user-identification local-authentication-table add user user1 ip-address
192.0.2.1 roles role1
```

```
user@host> request security user-identification local-authentication-table add user user2 ip-address
203.0.113.2 roles [role2 role3]
```

```
user@host> request security user-identification local-authentication-table add user user2 ip-address
203.0.113.2 roles role1
```

```
user@host> show security user-identification local-authentication-table all
```

```
Total entries: 2
Source IP       Username      Roles
192.0.2.1       user1      role1
203.0.113.2     user2      role2, role3, role1
```

request security user-identification local-authentication-table delete

Syntax

```
request security user-identification local-authentication-table delete ip-address | user-name
```

Release Information
Command introduced in Junos OS Release 12.1.

Description
This command removes an entry from the local authentication table. You can identify the entry by IP address or user-name. To change the user name of an entry or to remove or change entries in a role list, you must delete the existing entry and create a new one.

Options
ip-address—The IP address of the entry to be deleted.

user-name—The user name of the entry to be deleted. To change the user name of an entry, you must delete the old entry and create a new one.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

request security user-identification local-authorization-table add | 495
Understanding the User Identification Table | 186

Output Fields
The specified show command verifies the table content before and after an entry has been deleted from the local authentication table.

Sample Output

```
user@host> show security user-identification local-authentication-table all
```

```
Total entries: 2
    Ip-address: 192.0.2.1
    Username: user1
    Roles: role1

    Ip-address: 203.0.113.2
    Username: user2
    Roles: role2, role3, role1
```

user@host> **request security user-identification local-authentication-table delete 203.0.113.2**

user@host> **show security user-identification local-authentication-table all**

```
Total entries: 1
    Ip-address: 192.0.2.1
    Username: user1
    Roles: role1
```

show security alarms

Syntax

```
show security alarms
<detail>
<alarm-id id-number>
<alarm-type [ types ]>
<newer-than YYYY-MM-DD.HH:MM:SS>
<older-than YYYY-MM-DD.HH:MM:SS>
<process process>
<severity severity>
```

Release Information

Command introduced in Junos OS Release 11.2.

Description

Display the alarms that are active on the device. Run this command when the CLI prompt indicates that a security alarm has been raised, as shown here:

```
[1 SECURITY ALARM] user@host#
```

Options

none—Display all active alarms.

detail—(Optional) Display detailed output.

alarm-id *id-number*—(Optional) Display the specified alarm.

alarm-type [*types*]—(Optional) Display the specified alarm type or a set of types.

You can specify one or more of the following alarm types:

- **authentication**
- **cryptographic-self-test**
- **decryption-failures**
- **encryption-failures**
- **ike-phase1-failures**
- **ike-phase2-failures**
- **key-generation-self-test**
- **non-cryptographic-self-test**

- **policy**
- **replay-attacks**

newer-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Display active alarms that were raised after the specified date and time.

older-than *YYYY-MM-DD.HH:MM:SS*—(Optional) Display active alarms that were raised before the specified date and time.

process *process*—(Optional) Display active alarms that were raised by the specified system process.

severity *severity*—(Optional) Display active alarms of the specified severity.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

Required Privilege Level
security—To view this statement in the configuration.

RELATED DOCUMENTATION

clear security alarms

Example: Generating a Security Alarm in Response to Policy Violations

List of Sample Output
show security alarms on page 501
show security alarms detail on page 501
show security alarms alarm-id on page 502
show security alarms alarm-type authentication on page 502
show security alarms newer-than <time> on page 503
show security alarms older-than <time> on page 503
show security alarms process <process> on page 503

show security alarms severity <severity> on page 503

Output Fields

Table 35 on page 501 lists the output fields for the **show security alarms** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the **detail** keyword is used.

Table 35: show security alarms

Field Name	Field Description	Level of Output
ID	Identification number of the alarm.	All levels
Alarm time	Date and time the alarm was raised..	All levels
Message	Information about the alarm, including the alarm type, username, IP address, and port number.	All levels
Process	System process (For example, login or sshd) and process identification number associated with the alarm.	**detail**
Severity	Severity level of the alarm.	**detail**

Sample Output

show security alarms

```
[3 SECURITY ALARMS] user@router> show security alarms
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms detail

```
[3 SECURITY ALARMS] user@router> show security alarms detail
```

```
Alarm ID   : 1
Alarm Type : authentication
Time       : 2010-01-19 13:41:36 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 2
Alarm Type : authentication
Time       : 2010-01-19 13:41:52 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 3
Alarm Type : authentication
Time       : 2010-01-19 13:42:13 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2’
Process    : sshd (pid 1414)
Severity   : notice
```

show security alarms alarm-id

[3 SECURITY ALARMS] user@router> **show security alarms alarm-id 1**

```
ID    Alarm time              Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms alarm-type authentication

[3 SECURITY ALARMS] user@router> **show security alarms alarm-type authentication**

```
ID    Alarm time              Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
```

```
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms newer-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms newer-than 2010-01-19.13:41:59
```

```
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms older-than 2010-01-19.13:41:59
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> show security alarms process sshd
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

show security alarms severity <severity>

```
[3 SECURITY ALARMS] user@router> show security alarms severity notice
```

```
ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '203.0.113.2’
```

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 Junos OS Release 8.5. The **node** options added in Junos OS Release 9.0.

Description

Display information about the users at the specified IP address that are currently authenticated.

Options

- **address *ip-address***—IP address of the authentication source.
- none—Display all the firewall authentication information for users at this IP address.
- **node**—(Optional) For chassis cluster configurations, display user firewall authentication entries on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

Required Privilege Level

view

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

List of Sample Output

show security firewall-authentication users address 192.0.2.9 on page 506
show security firewall-authentication users address 192.0.2.9 node local on page 507
show security firewall-authentication users address 198.51.100.29 on page 507

Output Fields

Table 36 on page 506 lists the output fields for the **show security firewall-authentication users address** command. Output fields are listed in the approximate order in which they appear.

Table 36: 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.
Lsys	The logical system where the traffic was received.
Source zone	User traffic received from the zone.
Destination zone	User traffic destined to the zone.
Policy index	Identification number of the policy.
Policy name	Name of the policy.
Access profile	Name of profile used for authentication.
Interface Name	Name of the interface.
Bytes sent by this user	Number of bytes sent by the user.
Bytes received by this user	Number of bytes received by the user.
Client-groups	Name of the client group.

Sample Output

show security firewall-authentication users address 192.0.2.9

`user@host>` **show security firewall-authentication users address 192.0.2.9**

```
Username: hello
Source IP: 192.0.2.9
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: my-group1-example, my-group2-example
```

Sample Output

show security firewall-authentication users address 192.0.2.9 node local

`user@host>` **show security firewall-authentication users address 192.0.2.9 node local**

```
node0:
--------------------------------------------------------------------------
Username: local1
Source IP: 192.0.2.9
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 address 198.51.100.29

`user@host>` **show security firewall-authentication users address 198.51.100.29**

```
Username: hello
Source IP: 198.51.100.29/24
Authentication state: Success
Authentication method: User-firewall
```

```
Age: 0
Access time remaining: 10
Lsys: root-logical-system
Source zone: N/A
Destination zone: N/A
Access profile: test
```

show security firewall-authentication users auth-type

Syntax

```
show security firewall-authentication users auth-type [user-firewall | pass-through | web-authentication]
```

Release Information

Command introduced in Junos OS Release 12.1X45-D10

Description

Display statistics about the users authenticated by the selected method.

Options

- **user-firewall**—Lists all users authenticated for user firewall.
- **pass-through**—Lists all users authenticated by the pass-through method.
- **web-authentication**—Lists all users authenticated by the user authentication method.

Required Privilege Level

view

RELATED DOCUMENTATION

Understanding User Role Firewalls | 183

List of Sample Output

show security firewall-authentication users auth-type user-firewall on page 510
show security firewall-authentication users auth-type pass-through on page 510
show security firewall-authentication users auth-type pass-through on page 510

Output Fields

Table 37 on page 509 lists the output fields for the **show security firewall-authentication users auth-type** command. Output fields are listed in the approximate order in which they appear.

Table 37: show security firewall-authentication users auth-type Output Fields

Field Name	Field Description
Total users in table	Total number of users authenticated by this method.
Id	The ID assigned to the entry.

Table 37: show security firewall-authentication users auth-type Output Fields *(continued)*

Field Name	Field Description
Source IP	The source IP address of the traffic.
Src zone	The source zone of the traffic.
Dst zone	The destination zone of the traffic.
Profile	The profile used to authenticate the used.
Age	The length of time since authentication.
Status	The status of the authentication.
User	The username associated with the traffic.

Sample Output

show security firewall-authentication users auth-type user-firewall

```
user@host> show security firewall-authentication users auth-type user-firewall
```

```
User-firewall authentication data:
  Total users in table: 2
          Id Source Ip   Src zone Dst zone Profile    Age Status   User
           1 10.208.16.1  N/A      N/A      test        0 Success  jasonliu
           2 10.208.16.6  N/A      N/A      test6       0 Failed   jason
```

show security firewall-authentication users auth-type pass-through

```
user@host> show security firewall-authentication users auth-type pass-through
```

```
Pass-through firewall authentication data:
  Total users in table: 1
          Id Source Ip   Src zone Dst zone Profile    Age Status   User
           1 10.208.16.2  zone1    zone2    test2       0 Success  jasonliu2
```

show security firewall-authentication users auth-type pass-through

```
user@host> show security firewall-authentication users auth-type web-authentication
```

```
Web firewall authentication data:
  Total users in table: 1
          Id Source Ip   Src zone Dst zone Profile    Age Status   User
           1 10.208.16.3  N/A      N/A      test3       0 Success  jasonliu3
```

show security flow session application

Syntax

```
show security flow session application
application-name [brief | extensive | summary]
```

Release Information

Command introduced in Junos OS Release 8.5. Filter and view options added in Junos OS Release 10.2.

Description

Display information about each session of the specified application type.

Options

- ***application-name***—Type of application about which to display sessions information. Possible values are:
  - dns–Domain Name System
  - ftp–File Transfer Protocol
  - ignore–Ignore application type
  - mgcp-ca–Media Gateway Control Protocol with Call Agent
  - mgcp-ua–MGCP with User Agent
  - pptp–Point-to-Point Tunneling Protocol
  - q931–ISDN connection control protocol
  - ras–Remote Access Server
  - realaudio–RealAudio
  - rsh–UNIX remote shell services
  - rtsp–Real-Time Streaming Protocol
  - sccp–Skinny Client Control Protocol
  - sip–Session Initiation Protocol
  - sqlnet-v2–Oracle SQLNET
  - talk–TALK program
  - tftp–Trivial File Transfer Protocol
- brief | extensive | summary–Display the specified level of output.

Required Privilege Level

view

RELATED DOCUMENTATION

clear security flow session application

List of Sample Output

show security flow session application telnet on page 514
show security flow session application telnet brief on page 515
show security flow session application telnet extensive on page 515
show security flow session application telnet summary on page 516

Output Fields

Table 38 on page 513 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 38: show security flow session application Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.

Table 38: show security flow session application Output Fields *(continued)*

Field Name	Field Description
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

Sample Output

show security flow session application telnet

`root>` **show security flow session application telnet**

```
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes: 610
```

```
  Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes: 602
Total sessions: 1
```

show security flow session application telnet brief

root> **show security flow session application telnet brief**

```
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes: 610

  Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes: 602
Total sessions: 1
```

show security flow session application telnet extensive

root> **show security flow session application telnet extensive**

```
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1788
Session State: Valid
Start time: 670184, Duration: 33
   In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
```

```
    Route: 0x60010, Gateway: 203.0.113.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 192.0.2.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1
```

show security flow session application telnet summary

root> **show security flow session application telnet summary**

```
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security match-policies

Syntax

```
show security match-policies
destination-ip <ip-address>
destination-port < port-number>
from-zone <zone-name>
global
logical-system <logical-system-name>
protocol <protocol-name | protocol-number>
result-count <number>
root-logical-system
source-end-user-profile <device-identity-profile-name>
source-identity <role-name>
source-ip <ip-address>
source-port <port-number>
tenant <tenant-name>
to-zone <zone-name>
```

Release Information

Command introduced in Junos OS Release 10.3.
Command updated in Junos OS Release 10.4.
Command updated in Junos OS Release 12.1.
Command updated to include optional from-zone and to-zone global match options in Junos OS Release 12.1X47-D10.
The **tenant** option is introduced in Junos OS Release 18.3R1.

Description

The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, then the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are “shadowed” by the first and are never encountered by matching traffic.

> **NOTE:** The **show security match-policies** command is applicable only to security policies; IDP policies are not supported.

Options

- **destination-ip** ***destination-ip***—Displays the destination IP address of the traffic.
- **destination-port** ***destination-port***–Displays the destination port number of the traffic. Range is 1 through 65,535.
- **from-zone** ***zone-name***—Displays the name or ID of the source zone of the traffic.
- **global**—Displays information about global policies.
- **logical-system**—Displays the logical system name.
- **protocol** ***protocol-name*** **|** ***protocol-number***–Displays the protocol name or numeric value of the traffic.
  - **ah** or **51**
  - **egp** or **8**
  - **esp** or **50**
  - **gre** or **47**
  - **icmp** or **1**
  - **igmp** or **2**
  - **igp** or **9**
  - **ipip** or **94**
  - **ipv6** or **41**
  - **ospf** or **89**
  - **pgm** or **113**
  - **pim** or **103**
  - **rdp** or **27**
  - **rsvp** or **46**
  - **sctp** or **132**
  - **tcp** or **6**
  - **udp** or **17**
  - **vrrp** or **112**

- **result-count *number***—(Optional) Displays the number of policy matches. Valid range is from 1 through 16. The default value is 1.
- **root-logical-system**—Displays root logical system as default.
- **source-end-user-profile** *device-identity-profile-name*—(Optional) Displays the device identity profile that specifies characteristics that can apply to one or more devices.
- **source-identity *role-name***—(Optional) Displays the source identity of the traffic determined by the user role.
- **source-ip *source-ip***—Displays the source IP address of the traffic.
- **source-port *source-port***—Displays the source port number of the traffic. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone *zone-name***—Displays the name or ID of the destination zone of the traffic.

Required Privilege Level
view

RELATED DOCUMENTATION

clear security policies statistics | 488
Security Policies Overview | 23
Understanding Security Policy Rules | 106
Understanding Security Policy Elements | 105

List of Sample Output

Example 1: show security match-policies on page 521
Example 2: show security match policies ... result-count on page 521
Example 3: show security match policies ... source-identity on page 522
Example 4: show security match policies ... global on page 523
show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp on page 523

Output Fields

Table 39 on page 519 lists the output fields for the **show security match-policies** command. Output fields are listed in the approximate order in which they appear.

Table 39: show security match-policies Output Fields

Field Name	Field Description
Policy	Name of the applicable policy.

Table 39: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Action or **Action-type**	The action to be taken for traffic that matches the policy's match criteria. Actions include the following: • **permit** • **firewall-authentication** • **tunnel ipsec-vpn *vpn-name*** • **pair-policy *pair-policy-name*** • **deny** • **reject**
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	An internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.
From zone	Name of the source zone.
To zone	Name of the destination zone.
Source addresses	The names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it.
Application	Name of a preconfigured or custom application, or **any** if no application is specified.
IP protocol	Numeric value for the IP protocol used by the application, such as 6 for TCP or 1 for ICMP.
ALG	If an ALG is associated with the session, the name of the ALG. Otherwise, 0.

Table 39: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Inactivity timeout	Elapsed time without activity after which the application is terminated.
Source-port range	Range of matching source ports defined in the policy.
Destination-port range	Range of matching destination ports defined in the policy.
Source identities	One or more user roles defined in the matching policy.
global	Display information about global policies.
device-identity-profile-name	Device identity profile that specifies characteristics that can apply to one or more devices.

Sample Output

Example 1: show security match-policies

`user@host>` **show security match-policies from-zone z1 to-zone z2 source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp**

```
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 198.51.100.0/24
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 203.0.113.0/24
    d3: 192.0.2.1/32
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [21-21]
```

Example 2: show security match policies ... result-count

`user@host>` **show security match-policies from-zone zone-A to-zone zone-B source-ip 10.10.10.1 destination-ip 192.0.2.5 source_port 1004 destination_port 80 protocol tcp result_count 5**

```
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 192.0.2.0/24
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
  Sequence number: 15
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa11: 10.10.10.1/32
  Destination addresses:
    da15: 192.0.2.5/32
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]
```

Example 3: show security match policies ... source-identity

`user@host>` **show security match-policies from-zone untrust to-zone trust source-ip 10.10.10.1 destination-ip 192.0.2.1 destination_port 21 protocol 6 source-port 1234 source-identity role1**

```
Policy: p1, action-type: permit, State: enabled, Index: 40
      Policy Type: Configured
      Sequence number: 1
      From zone: untrust, To zone: trust
      Source addresses:
        a1: 10.0.0.0/8
      Destination addresses:
        d1: 192.0.2.0/24
      Application: junos-ftp
        IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
          Source port range: [0-0]
          Destination port range: [21-21]
      Source identities: role1
      Per policy TCP Options: SYN check: No, SEQ check: No
```

Example 4: show security match policies ... global

`user@host>` **show security match-policies global source-ip 10.10.10.1 destination-ip 192.0.2.5 source_port 1004 destination_port 80 protocol tcp result_count 5**

```
Policy: gp1, action-type: permit, State: enabled, Index: 6, Scope Policy: 0
  Policy Type: Configured, global
  Sequence number: 1
  From zones:
    Any
  To zones:
    Any
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp

`user@host>` **show security match-policies tenant TN1 from-zone trust to-zone untrust source-ip 10.10.10.1 destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp**

```
Policy: p1, action-type: permit, State: enabled, Index: 4
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
a2: 198.51.100.0/24
a3: 10.10.10.1/32
Destination addresses:
d2: 203.0.113.0/24
d3: 192.0.2.1/32
Application: junos-ftp
IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [21-21]
```

show security policies

Syntax

```
show security policies
<all-logical-systems-tenants>
<checksum>
<count>
<detail>
<from-zone zone-name>
<global>
<hit-count>
<information>
<logical-system logical-system-name>
<policy-name policy-name>
<root-logical-system>
<service-set>
<start>
<tenant tenant-name>
<to-zone zone-name>
<unknown-source-identity>
<zone-context>
```

Release Information

Command modified in Junos OS Release 9.2.
Support for IPv6 addresses is added in Junos OS Release 10.2.
Support for wildcard addresses is added in Junos OS Release 11.1.
Support for global policy and services offloading is added in Junos OS Release 11.4.
Support for source-identities and the **Description** output field is added in Junos OS Release 12.1.
Support for negated address added in Junos OS Release 12.1X45-D10.
The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options are expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options is added in Junos OS Release 12.3X48-D20.
Output field and description for **source-end-user-profile** option is added in Junos OS Release 15.1x49-D70.
Output field and description for **dynamic-applications** option is added in Junos OS Release 15.1x49-D100.
Output field and description for **dynapp-redir-profile** option is added in Junos OS Release 18.2R1.
The **tenant** option is introduced in Junos OS Release 18.3R1.
The **<all-logical-systems-tenants>** option is introduced in Junos OS Release 18.4R1.
The **information** option is introduced in Junos OS Release 18.4R1.
The **checksum** option is introduced in Junos OS Release 18.4R1.

Description

Displays a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy. The existing show commands for displaying the policies configured with multiple tenant support are enhanced. A security policy controls the traffic flow from one zone to another zone. The security policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another.

Options

- **all-logical-systems-tenants**—Displays all multitenancy systems.
- **checksum**—Displays the policy information checksum.
- **count**—Displays the number of policies to show. Range is 1 through 65,535.
- **detail**—(Optional) Displays a detailed view of all of the policies configured on the device.
- **from-zone**—Displays the policy information matching the given source zone.
- **global**—(Optional) Displays the policy information about global policies.
- **hit-count**—Displays the policies hit count.
- **information**—Displays the policy information.
- **logical-system**—Displays the logical system name.
- **policy-name**—(Optional) Displays the policy information matching the given policy name.
- **root-logical-system**—Displays root logical system as default.
- **service-set**—Displays the name of the service set.
- **start**—Displays the policies from a given position. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone**—Displays the policy information matching the given destination zone.
- **unknown-source-identity**—Displays the unknown-source-identity of a policy.
- **zone-context**—Displays the count of policies in each context (from-zone and to-zone).

Required Privilege Level

view

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Rules | 106

Understanding Security Policy Elements | 105

Unified Policies Configuration Overview | 146

List of Sample Output

show security policies on page 530
show security policies (Dynamic Applications) on page 530
show security policies policy-name detail on page 531
show security policies (Services-Offload) on page 533
show security policies (Device Identity) on page 533
show security policies detail on page 534
show security policies detail (TCP Options) on page 537
show security policies policy-name (Negated Address) on page 537
show security policies policy-name detail (Negated Address) on page 538
show security policies global on page 538
show security policies detail tenant on page 539

Output Fields

Table 40 on page 526 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 40: 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	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.

Table 40: 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. 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.
source-end-user-profile	Name of the device identity profile (referred to as **end-user-profile** in the CLI) that contains attributes, or characteristics of a device. Specification of the device identity profile in the **source-end-user-profile** field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device.
Source addresses (excluded)	Name of the source address excluded from the policy.
Destination addresses (excluded)	Name of the destination address excluded from the policy.
Source identities	One or more user roles specified for a policy.
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The Internet protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, **ignore** is displayed. Otherwise, **0** is displayed. However, even if this command shows **ALG: 0**, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications. • **Inactivity timeout**: Elapsed time without activity after which the application is terminated. • **Source port range**: The low-high source port range for the session application.
Dynamic Applications	Application identification-based Layer 7 dynamic applications.

Table 40: show security policies Output Fields *(continued)*

Field Name	Field Description
Destination Address Translation	Status of the destination address translation traffic: • **drop translated**—Drop the packets with translated destination addresses. • **drop untranslated**—Drop the packets without translated destination addresses.

Application Firewall	An application firewall includes the following:
	• **Rule-set**—Name of the rule set.
	• **Rule**—Name of the rule.
	  ◦ **Dynamic applications**—Name of the applications.
	  ◦ **Dynamic application groups**—Name of the application groups.
	  ◦ **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ▪ **permit**
	  ▪ **deny**
	• **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set.

Action or Action-type	• The action taken for 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**
	  ◦ **services-offload**

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 and can be used as a possible match for traffic.

Table 40: show security policies Output Fields *(continued)*

Field Name	Field Description

Policy statistics	• **Input bytes**—The total number of bytes presented for processing by the device.
	  ◦ **Initial direction**—The number of bytes presented for processing by the device from the initial direction.
	  ◦ **Reply direction**—The number of bytes presented for processing by the device from the reply direction.
	• **Output bytes**—The total number of bytes actually processed by the device.
	  ◦ **Initial direction**—The number of bytes from the initial direction actually processed by the device.
	  ◦ **Reply direction**—The number of bytes from the reply direction actually processed by the device.
	• **Input packets**—The total number of packets presented for processing by the device.
	  ◦ **Initial direction**—The number of packets presented for processing by the device from the initial direction.
	  ◦ **Reply direction**—The number of packets presented for processing by the device from the reply direction.
	• **Output packets**—The total number of packets actually processed by the device.
	  ◦ **Initial direction**—The number of packets actually processed by the device from the initial direction.
	  ◦ **Reply direction**—The number of packets actually processed by the device from the reply direction.
	• **Session rate**—The total number of active and deleted sessions.
	• **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**—The number of times the policy was accessed to check for a match.

dynapp-redir-profile	Displays unified policy redirect profile. See profile(dynamic-application).
Per policy TCP Options	Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both.

Sample Output

show security policies

user@host> **show security policies**

```
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
  Source addresses:
  sa-1-ipv4: 198.51.100.11/24
  sa-2-ipv6: 2001:db8:a0b:12f0::1/32
  sa-3-ipv6: 2001:db8:a0b:12f0::22/32
  sa-4-wc:   203.0.113.1/255.255.0.255
  Destination addresses:
  da-1-ipv4: 2.2.2.2/24
  da-2-ipv6: 2001:db8:a0b:12f0::8/32
  da-3-ipv6: 2001:db8:a0b:12f0::9/32
  da-4-wc:   192.168.22.11/255.255.0.255
  Source identities: role1, role2, role4
  Applications: any
  Action: permit, application services, log, scheduled
  Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
  Source addresses:
  sa-1-ipv4:  198.51.100.11/24
  sa-2-ipv6:  2001:db8:a0b:12f0::1/32
  sa-3-ipv6:  2001:db8:a0b:12f0::22/32
  Destination addresses:
  da-1-ipv4:  2.2.2.2/24
  da-2-ipv6:  2001:db8:a0b:12f0::1/32
  da-3-ipv6:  2001:db8:a0b:12f0::9/32
  Source identities: role1, role4
  Applications: any
  Action: deny, scheduled
```

show security policies (Dynamic Applications)

user@host>**show security policies**

```
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
  Source addresses: any
  Destination addresses: any
```

```
    Applications: any
    Dynamic Applications: junos:YAHOO
    Action: deny, log
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:web, junos:web:social-networking:facebook,
    junos:TFTP, junos:QQ
    Action: permit, log
  Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:HTTP, junos:SSL
    Action: permit, application services, log
```

The following example displays the output with unified policies configured.

`user@host>` **show security policies**

```
Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
  Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
    dynapp-redir-profile: profile1
```

show security policies policy-name detail

`user@host>` **show security policies policy-name p1 detail**

```
  Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    sa-1-ipv4:  198.51.100.11/24
```

```
    sa-2-ipv6:  2001:db8:a0b:12f0::1/32
    sa-3-ipv6:  2001:db8:a0b:12f0::9/32
    sa-4-wc:    203.0.113.1/255.255.0.255
  Destination addresses:
    da-1-ipv4: 192.0.2.0/24
    da-2-ipv6: 2001:db8:a0b:12f0::1/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
    da-4-wc:   192.168.22.11/255.255.0.255
Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Destination Address Translation: drop translated
  Application firewall :
  Rule-set: my_ruleset1
    Rule: rule1
      Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
      Dynamic Application groups: junos:web, junos:chat
      Action: deny
    Default rule: permit
  Session log: at-create, at-close
  Scheduler name: sch20
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes       :               18144                 545 bps
      Initial direction:                9072                272 bps
      Reply direction  :                9072                 272 bps
    Output bytes       :               18144                 545 bps
      Initial direction:                9072                 272 bps
      Reply direction  :                9072                 272 bps
    Input  packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
    Output packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
    Session rate       :                 108                   3 sps
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
```

The following example displays the output with unified policies configured.

user@host> **show security policies policy-name p1 detail**

```
Default policy: permit-all
Pre ID default policy: permit-all
From zone: trust, To zone: trust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: reject
    dynapp-redir-profile: profile1
```

show security policies (Services-Offload)

user@host> **show security policies**

```
  Policy: p1, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies (Device Identity)

user@host> **show security policies**

```
From zone: trust, To zone: untrust
      Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0, Sequence
```

```
 number: 1
         Source addresses: any
         Destination addresses: any
         source-end-user-profile: marketing-profile
         Applications: any
         Action: permit
```

show security policies detail

user@host> **show security policies detail**

```
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
 4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes       :               18144                 545 bps
      Initial direction:                9072                272 bps
      Reply direction  :                9072                 272 bps
    Output bytes       :               18144                 545 bps
      Initial direction:                9072                 272 bps
      Reply direction  :                9072                 272 bps
    Input  packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
```

```
    Output packets     :                 216                   6 pps
      Initial direction:                 108                   3 bps
      Reply direction  :                 108                   3 bps
    Session rate       :                 108                   3 sps
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p2 is for the sales team
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

The following example displays the output with unified policies configured.

`user@host>` **show security policies detail**

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
```

```
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: junos-defaults
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [443-443]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [5432-5432]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [80-80]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [3128-3128]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8000-8000]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8080-8080]
  IP protocol: 17, ALG: 0, Inactivity timeout: 60
    Source port range: [0-0]
    Destination port range: [1-65535]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [443-443]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [5432-5432]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [80-80]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [3128-3128]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8000-8000]
  IP protocol: 6, ALG: 0, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [8080-8080]
  IP protocol: 17, ALG: 0, Inactivity timeout: 60
    Source port range: [0-0]
```

```
      Destination port range: [1-65535]
  Dynamic Application:
    junos:FACEBOOK-CHAT: 10704
    junos:GMAIL: 51
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies detail (TCP Options)

user@host> **show security policies policy-name p2 detail**

```
node0:
--------------------------------------------------------------------------
Policy:p2, action-type:permit, State: enabled,Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: tcp, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
 Destination port range: [80-80]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Dynamic-application: junos:HTTP
```

show security policies policy-name (Negated Address)

user@host> **show security policies policy-name p1**

```
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses(excluded): as1
    Destination addresses(excluded): as2
    Applications: any
    Action: permit
```

show security policies policy-name detail (Negated Address)

```
user@host> show security policies policy-name p1 detail
```

```
node0:
--------------------------------------------------------------------------
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
    ad1(ad): 255.255.255.255/32
    ad2(ad):  198.51.100.1/24
    ad3(ad):  198.51.100.6  ~ 198.51.100.56
    ad4(ad):  192.0.2.8/24
    ad5(ad):  198.51.100.99 ~ 198.51.100.199
    ad6(ad):  203.0.113.9/24
    ad7(ad):  203.0.113.23/24
  Destination addresses(excluded):
    ad13(ad2): 198.51.100.76/24
    ad12(ad2): 198.51.100.88/24
    ad11(ad2): 192.0.2.23 ~ 192.0.2.66
    ad10(ad2): 192.0.2.93
    ad9(ad2):  203.0.113.76 ~ 203.0.113.106
    ad8(ad2):  203.0.113.199
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

show security policies global

```
user@host> show security policies global policy-name Pa
```

```
node0:
--------------------------------------------------------------------------
  Global policies:
  Policy: Pa, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: H0
    Destination addresses: H1
    Applications: junos-http
```

```
    Action: permit
```

show security policies detail tenant

`user@host>` **show security policies detail tenant TN1**

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: junos-ping
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input  bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Output bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Input  packets   :                   0                   0 pps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Output packets   :                   0                   0 pps
Initial direction:                   0                   0 bps
```

```
Reply direction  :                 0                   0 bps
Session rate     :                 0                   0 sps
Active sessions  :                 0
Session deletions:                 0
Policy lookups   :                 0
```

show security policies checksum

Syntax

```
show security policies checksum
<logical-system (logical-system name | all)>
<root-logical-system>
<tenant tenant-name>
```

Release Information

Command introduced in Junos OS Release 18.4R1.

Description

Displays the security policy checksum value.

Verifying the checksum helps in validating the security policy sync status between the Routing Engine and the Packet Forwarding Engine. The checksum value should be the same for the Routing Engine and the Packet Forwarding Engine. If the checksum value is not same, then the different values indicates that the security policies on the Routing Engine and the Packet Forwarding Engine are out-of-sync.

> **NOTE:** The **show security policies checksum** command can only be used to ensure if the security policies are out of sync but cannot confirm if they are in-sync. Use the **request security policies check** command to get a list of all polices in-sync and/or out-of-sync.
>
> Use the **request security policies resync** command to synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine.

Options

logical-system (*logical-system-name* | all)—Displays the security policy checksum value for the security policies configured on a logical system or on all logical systems.

root-logical-system—Displays the security policy checksum value for the security policies configured on the root logical system. This is the default outcome.

tenant *tenant-name*—Displays the security policy checksum value for the security policies configured on a tenant.

Additional Information

The checksum value is a 32-character hexadecimal number that is computed for the security policy on the device.

Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.
- An error with the routing engine, such as a reused policy UID.

When the policy configuration are modified and the policies are out of sync, the following error message displays - **error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)>. Please request security policies check/resync**.

Required Privilege Level
view

RELATED DOCUMENTATION

request security policies check | 490
request security policies resync | 493

List of Sample Output
show security policies checksum (RE) on page 542
show security policies checksum (PFE) on page 542
show security policies checksum logical-system all on page 543

Sample Output

show security policies checksum (RE)

`user@host>` **show security policies checksum**

```
Logical system: root-logical-system
    From zone          To zone           Checksum
    trust              untrust           0xe0fc5791-d7ec5b89-cbc66724-35d706c
```

show security policies checksum (PFE)

`FLOWD_OCTEON(vty)#` **show usp policy checksum**

```
Logical system: root-logical-system
    From zone          To zone           Checksum
    trust              untrust           0xe0fc5791-d7ec5b89-cbc66724-35d706c
```

show security policies checksum logical-system all

user@host> **show security policies checksum logical-system all**

```
Logical system: LSYS1
    From zone          To zone           Checksum
    lsys1-trust        lsys1-untrust     0x7ff147ff-f9df0820-081fb02e-226455e3

Logical system: LSYS2
    From zone          To zone           Checksum
    lsys2-trust        lsys2-untrust     0x4bfd47fa-64fbb3e7-3a9444b5-94dd9db5
```

show security policies hit-count

Syntax

```
show security policies hit-count
<ascending>
<descending>
<from-zone zone-name>
<greater-than count>
<less-than count>
<logical-system (logical-system-name | all)>
<root-logical-system>
<tenant (tenant-name | all)>
<to-zone zone-name>
```

Release Information

Command introduced in Junos OS Release 12.1.
The **index** output field is added to the **show security policies hit-count** command to display the number of sessions redirected in Junos OS Release 18.2R1.
The **tenant** option is introduced in Junos OS Release 18.3R1.

Description

Display the utility rate of security policies according to the number of hits they receive. The number of hits can be listed without an order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

In a cluster, the count is a sum of all the Services Processing Cards (SPC) hit counts; it is cluster-wide. If a Packet Forwarding Engine (PFE) in a node is in failover mode, but does not reboot, the counter persists. If a node reboots, the PFE in the node also reboots, and the counter is cleared. During an in-service software upgrade (ISSU), all PFEs reboot, therefore all counters are cleared.

Use this command without options to display the number of hits in random order for all security policies and for all zones.

Options

- **ascending**—(Optional) Displays the number of hits for security policies in ascending order.
- **descending**—(Optional) Displays the number of hits for security policies in descending order.
- **from-zone *zone-name***—(Optional) Displays the number of hits for security policies associated with the named source zone.
- **greater-than *count***—(Optional) Displays security policies for which the number of hits is greater than the specified number.

Range: 0 through 4,294,967,295

- **less-than *count***—(Optional) Displays security policies for which the number of hits is less than the specified number.

  Range: 0 through 4,294,967,295

- **logical-system**—Displays the logical system name.
- **root-logical-system**—Displays root logical system as default.
- **tenant**—Displays the name of the tenant system.
- **to-zone *zone-name***—(Optional) Displays the number of hits for security policies associated with the named destination zone.

Required Privilege Level
view

RELATED DOCUMENTATION

clear security policies hit-count | 487
Security Policies Overview | 23
Unified Policies Configuration Overview | 146

List of Sample Output
show security policies hit-count on page 546
show security policies hit-count ascending on page 546
show security policies hit-count descending greater-than 70 less-than 100 on page 547
show security policies hit-count from-zone untrust to-zone trust on page 547
show security policies hit-count tenant all on page 547

Output Fields
Table 41 on page 545 lists the output fields for the **show security policies hit-count** command. Output fields are listed in the approximate order in which they appear.

Table 41: show security policies hit-count Output Fields

Field Name	Field Description
index	Displays the policy sequence number
from-zone	Name of the source zone
to-zone	Name of the destination zone

Table 41: show security policies hit-count Output Fields *(continued)*

Field Name	Field Description
name	Name of the security policy
policy count	Number of hits for each security policy
tenant	Displays the name of the tenant system.

Sample Output

show security policies hit-count

```
user@host> show security policies hit-count
```

```
index   from zone    to zone       name       policy count
 1       untrust      vrtrust      policy1         40
 2       untrust      trust        policy2         20
 3       untrust      trust        policy3         80

Number of policy: 3
```

Sample Output

show security policies hit-count ascending

```
user@host> show security policies hit-count ascending
```

```
index   from zone    to zone       name       policy count
 2       untrust      trust        policy2         20
 1       untrust      vrtrust      policy1         40
 3       untrust      trust        policy3         80

Number of policy: 3
```

Sample Output

show security policies hit-count descending greater-than 70 less-than 100

```
user@host> show security policies hit-count descending greater-than 70 less-than 100
```

```
index   from zone    to zone       name       policy count
 2       untrust      trust        policy2         100
 1       untrust      vrtrust      policy1         90
 3       untrust      trust        policy3         80

Number of policy: 3
```

Sample Output

show security policies hit-count from-zone untrust to-zone trust

```
user@host> show security policies hit-count from-zone untrust to-zone trust
```

```
index   from zone    to zone       name       policy count
 2       untrust      trust        policy2         20
 3       untrust      trust        policy3         80

Number of policy: 2
```

Sample Output

show security policies hit-count tenant all

```
user@host> show security policies hit-count tenant all
```

```
Tenant: TN1
Index   From zone        To zone          Name          Policy count
1       trust            untrust          p12           14
2       trust            untrust          p11           0

Number of policy: 2
```

show security policies information

Syntax

```
show security policies information
<logical-system (logical-system-name | all)>
<root-logical-system>
<tenant tenant-name>
```

Release Information

Command introduced in Junos OS Release 18.4R1.

Description

Displays detailed information about the security policies configured on the device.

> **NOTE:** Dynamic policy counters are only supported in the root logical system.

Options

logical-system—Displays detailed information about the security policies configured on a logical system or on all logical systems.

root-logical-system—Displays detailed information about the security policies configured on the root logical system. This is the default option.

tenant—Displays detailed information about the security policies configured on a tenant.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring Security Policies | 105

Unified Security Policies | 145

List of Sample Output

show security policies information on page 551

show security policies information logical-system all on page 552

Output Fields

Table 40 on page 526 lists the output fields for the **show security policies information** command. Output fields are listed in the approximate order in which they appear.

Table 42: show security policies Output Fields

Field Name	Field Description
Number of global policies	Number of global policies configured on the device.
Number of policies with scheduler	Number of policies with schedulers configured on the device.
Number of policies with statistics enabled	Number of policies configured with statistics enabled on the device and the maximum number of policies which can be configured with statistics enabled on the device.
Number of unified policies	Number of unified policies configured on the device.
Number of policy contexts	Number of policy contexts configured on the device.
Number of Policies per context	Number of policies per context configured on the device and the maximum number of policies per context that can be configured on the device.
Number of Source addresses per policy	Number of source addresses configured per policy and the maximum number of source addresses configured per policy. The source address in the match criteria is composed of one or more address names or address set names in the **from-zone**.
Number of Destination addresses per policy	Number of destination addresses configured per policy and maximum of destination addresses that can be configured per policy. The destination address of the match criteria is composed of one or more address names or address set names in the **to-zone**.
Number of Applications per policy	Number of applications per policy and the maximum number of applications per policy.
Number of Dynamic applications per policy	Number of dynamic applications per policy and the maximum number of dynamic applications per policy.
Number of Source identities per policy	Number of source identities per policy and the maximum number of source identities per policy.
Messages received	Number of messages received.

Table 42: show security policies Output Fields *(continued)*

Field Name	Field Description
Messages rejected	Number of messages rejected.
Add messages received	Number of add messages received.
Delete messages received	Number of delete messages received.
Clear messages received	Number of clear messages received.
Invalid messages received	Number of invalid messages received.
Add messages sent to PFE	Number of add messages sent from Routing Engine to Packet Forwarding Engine.
Delete messages sent to PFE	Number of delete messages sent from Routing Engine to Packet Forwarding Engine.
Clear messages sent to PFE	Number of clear messages sent from Routing Engine to Packet Forwarding Engine.
Policy added successfully	Number of policies successfully added.
Policy deleted successfully	Number of policies successfully deleted.
Policy cleared successfully	Number of policies successfully cleared.
Policy add failures	Number of policies unsuccessfully added.
Policy delete failures	Number of policies unsuccessfully deleted.
Policy clear failures	Number of policies unsuccessfully cleared.
SSAM send attempted	Number of SSAM message attempts sent to Internet Key Exchange Protocol Daemon (IKED).
SSAM send succeeded	Number of SSAM messages sent to IKED.
SSAM send failed	Number of SSAM messages unsucessfully sent to IKED.
Policy failures - bad configuration	Number of messages with invalid dynamic policy configurations provided.
Policy failures - bad scope policy	Number of messages with invalid scope policy provided.
Dependent-dynamic-application-lookup	Value of the unified policy dependent match flag's value (**Dependent-dynamic-application-lookup**).

Table 42: show security policies Output Fields *(continued)*

Field Name	Field Description
Unified-policy-implicit-match	Value of the unified policy implicit match flag's value (**Unified-policy-implicit-match**).

Sample Output

show security policies information

`user@host>` **show security policies information**

```
  Number of policies                          :           0 / 16000
      Number of global policies               :           0
      Number of policies with scheduler       :           0
      Number of policies with statistics enabled:         0 / 256
      Number of unified policies              :           0
  Number of policy contexts                   :           0 / 4096
  Number of Policies per context              :           0 / 10240
  Number of Source addresses per policy       :           0 / 4096
  Number of Destination addresses per policy  :           0 / 4096
  Number of Applications per policy           :           0 / 3072
  Number of Dynamic applications per policy   :           0 / 4096
  Number of Source identities per policy      :           0 / 128

Dynamic policy counters:
  Messages received                 :           0
  Messages rejected                 :           0
  Add messages received             :           0
  Delete messages received          :           0
  Clear messages received           :           0
  Invalid messages received         :           0
  Add messages sent to PFE          :           0
  Delete messages sent to PFE       :           0
  Clear messages sent to PFE        :           0
  Policy added successfully         :           0
  Policy deleted successfully       :           0
  Policy cleared successfully       :           0
  Policy add failures               :           0
  Policy delete failures            :           0
  Policy clear failures             :           0
```

```
    SSAM send attempted                :           0
    SSAM send succeeded                :           0
    SSAM send failed                   :           0
    Policy failures - bad configuration :           0
    Policy failures - bad scope policy  :           0
Unified policy status:
  Dependent-dynamic-application-lookup: disable
  Unified-policy-implicit-match: enable
```

show security policies information logical-system all

user@host> **show security policies information logical-system all**

```
   Policy utilization counters:
    Number of policies                          :          10 / 60000
        Number of global policies               :           0
        Number of policies with scheduler       :           0
        Number of policies with statistics enabled:         0 / 1024
        Number of unified policies              :           1
    Number of policy contexts                   :           2 / 4096
    Number of Policies per context              :           9 / 60000
    Number of Source addresses per policy       :           4 / 4096
    Number of Destination addresses per policy  :           4 / 4096
    Number of Applications per policy           :           8 / 3072
    Number of Dynamic applications per policy   :          10 / 4096
    Number of URL Category per policy           :           0 / 1024
    Number of Source identities per policy      :           0 / 128

  Dynamic policy counters:
    Messages received                  :           0
    Messages rejected                  :           0
    Add messages received              :           0
    Delete messages received           :           0
    Clear messages received            :           0
    Invalid messages received          :           0
    Add messages sent to PFE           :           0
    Delete messages sent to PFE        :           0
    Clear messages sent to PFE         :           0
    Policy added successfully          :           0
    Policy deleted successfully        :           0
    Policy cleared successfully        :           0
    Policy add failures                :           0
    Policy delete failures             :           0
```

```
    Policy clear failures               :           0
    SSAM send attempted                 :           0
    SSAM send succeeded                 :           0
    SSAM send failed                    :           0
    Policy failures - bad configuration :           0
    Policy failures - bad scope policy  :           0
Unified policy status:
  Dependent-dynamic-application-lookup: disable
  Unified-policy-implicit-match: enable

Logical system: lsys1
  Policy utilization counters:
    Number of policies                            :           1 / 60000
        Number of global policies                 :           0
        Number of policies with scheduler         :           0
        Number of policies with statistics enabled:           0 / 1024
        Number of unified policies                :           0
    Number of policy contexts                     :           1 / 4096
    Number of Policies per context                :           1 / 60000
    Number of Source addresses per policy         :           1 / 4096
    Number of Destination addresses per policy    :           1 / 4096
    Number of Applications per policy             :           1 / 3072
    Number of Dynamic applications per policy     :           0 / 4096
    Number of URL Category per policy             :           0 / 1024
    Number of Source identities per policy        :           0 / 128
Unified policy status:
  Dependent-dynamic-application-lookup: disable
  Unified-policy-implicit-match: enable
```

show security policies unknown-source-identity

Syntax

```
show security policies unknown-source-identity
```

Release Information

Command introduced in Junos OS Release 12.1X45-D10.

Description

Display a list of any user or role that is referenced in a policy as a source-identity, but is not yet included in the role provisioning table.

The role provisioning table is created from the local authentication table, UAC authentication tables, and firewall authentication tables. The UAC and firewall authentication tables are dynamic and contain only those users currently authenticated. Because of this, a role can be listed as unknown because no user associated with the role has authenticated yet. There is no consequence if a role remains unknown.

Required Privilege Level

view

RELATED DOCUMENTATION

Security Policies Overview | 23

List of Sample Output

show security policies unknown-source-identity on page 555

Output Fields

Table 43 on page 554 lists the output fields for the **show security policies unknown-source-identity** command. Output fields are listed in the approximate order in which they appear.

Table 43: show security policies unknown-source-identity Output Fields

Field Name	Field Description
From zone	Part of the zone pair that identifies the source of the traffic to which a policy applies. Affected policies are grouped by their zone pair.
To zone	Part of the zone pair that identifies the destination of the traffic to which a policy applies. Affected policies are grouped by their zone pair.
Policy	The name of the policy that contains the unknown source identity.

Table 43: show security policies unknown-source-identity Output Fields *(continued)*

Field Name	Field Description
Unknown source identities	A list of user names and roles specified in the source-identity field of the named policy that are unknown.

Sample Output

show security policies unknown-source-identity

In the following sample output, policy p1 which controls traffic from the untrust zone to the trust zone specifies two roles, r1 and r3, that are not yet provisioned. Similarly, policy p2 affecting traffic from the trust zone to the trust zone also contains two roles that are not provisioned, role1 and abc.

`user@host>` **show security policies unknown-source-identity**

```
From zone: untrust, To zone: trust
  Policy: p1
  Unknown source identities: r1, r3
From zone: trust, To zone: trust
  Policy: p2
  Unknown source identities: role1, abc
```

show security policies zone-context

Syntax

```
show security policies zone-context
application-firewall
count
detail
from-zone <zone-name>
interface
logical-system <logical-system-name>
policy-name
root-logical-system
service-set
start
tenant <tenant-name>
to-zone <zone-name>
```

Release Information

Command introduced in Junos OS Release 8.5.
The **tenant** option is introduced in Junos OS Release 18.3R1.

Description

Displays the security policy that applies the security rules to the transit traffic within a context (from-zone to to-zone). From the perspective of security policies, traffic enters into one security zone and goes out on another security zone. This combination of a **from-zone** and a **to-zone** is defined as a context. Each context contains an ordered list of policies. The existing show command for security policies zone-context is enhanced with tenant support.

Options

application-firewall—Displays the information of application-firewall.

count—Displays the number of policies to show.

Range: 1 through 65535

detail—Displays the detailed information.

from-zone—Displays the policy information matching the given source zone.

interface—Displays the name of adaptive services interface.

logical-system—Displays the name of the logical system.

policy-name—Displays the policy information matching the given policy name.

root-logical-system—Displays root logical system as default.

service-set—Displays the name of service set.

start—Displays the policies from a given position.

Range: 1 through 65535

tenant—Displays the name of the tenant system.

to-zone—Displays the policy information matching the given destination zone.

Required Privilege Level
view

RELATED DOCUMENTATION

Security Policies Overview | 23

Understanding Security Policy Rules | 106

List of Sample Output

show security policies zone-context tenant TN1 on page 558
show security policies zone-context tenant all on page 558

Output Fields

Table 39 on page 519 lists the output fields for the **show security policies zone-context** command. Output fields are listed in the approximate order in which they appear.

Table 44: show security zone-context Output Fields

Field Name	Field Description
From zone	Name or ID of the source zone of the traffic.
To zone	Name or ID of the destination zone of the traffic.
Policy count	Number of hits for each security policy.
Tenant	Name of the tenant system.

Sample Output

show security policies zone-context tenant TN1

`user@host>` **show security policies zone-context tenant TN1**

```
From zone               To zone                 Policy count
   z1                       z2                      1
   z2                       z3                      1
```

show security policies zone-context tenant all

`user@host>` **show security policies zone-context tenant all**

```
Tenant: TN1
    From zone               To zone                 Policy count
    z1                      z2                      1

Tenant: TN2
    From zone               To zone                 Policy count
    z1                      z2                      1
```

show security policy-report

Syntax

```
show security policy-report
<from-zone zone-name>
<global>
<report-type report-type>
<to-zone zone-name>
```

Release Information

Command introduced in Junos OS Release 20.1R1.

Description

Displays detailed security policy reports.

Optimizing security policies ensure that the policies are efficient. Over time, policies become disorganised and hence ineffective. You can use the **show security policy-report** command to notify end users when you create new policies or change existing policies which adversely affect other security policies.

Options

from-zone—Displays the policy report matching the given source zone.

Default: any

global—Displays the security policy report of the global policies.

report-type—Displays the type of the policy report.

You can configure the following options for **report-type**:

1-year-not-hit—Displays the policy report for policies that have not been hit in the last 1 year.

30d-not-hit—Displays the policy report for policies that have not been hit in the last 30 days.

60d-not-hit—Displays the policy report for policies that have not been hit in the last 60 days.

90d-not-hit—Displays the policy report for policies that have not been hit in the last 90 days.

consolidation—Displays the policy report for policies which can be consolidated.

When two policies share most fields in common and only one of the fields contains difference, they are eligible for consolidation.

expired—Displays the policy report for expired policies.

generalization—Displays the policy report for generalized policies.

A policy is generalized when a following policy matches all the packets of the current policy and the action for each policy is different.

least-hit—Displays the policy report for policies with the least hit count.

most-hit—Displays the policy report for policies with the most hit count.

no-comments—Displays the policy report for policies which have no comments.

no-logging—Displays the policy report for policies which do not have any logging

redundant—Displays the policy report for redundant policies.

A policy is redundant if there exists a preceding policy within the policy which performs the same action on the same packets as performed by the current policy.

scheduler—Displays the policy report for policies in which the scheduled has expired/policies that have an active or inactive schedule.

shadowing—Displays the policy report for shadowed policies.

A policy is shadowed when a preceding policy matches all the packets of the current policy and the action for each policy is different.

unused—Displays the policy report for policies which have a hit count value of zero.

Default: If you don't configure a specific **report-type**, then all the reports are displayed.

to-zone—Displays the policy report matching the given destination zone.

Default: any

NOTE: SRX series devices only analyze the following fields of a policy for the shadowing, redundant, generalization, and consolidation reports:

- Source address (Ipv4 only)
- Destination address (Ipv4 only)
- Applications

Required Privilege Level

view

RELATED DOCUMENTATION

report-skip | 408

Sample Output

show security policy-report report-type consolidation

`user@host>` **show security policy-report report-type consolidation**

```
Logical system: root-logical-system
  Problem: Policy p2 is consolidated with policy p1
  Recommendation: Please check if policy p2 and p1
    Index: 129
    Policy: p2
      Source zone: trust
      Destination zone: untrust
      Source addresses: s_ad2
      Destination addresses: d_ad2
      Applications: app2
      Action: permit

    Policy: p1
      Source zone: trust
      Destination zone: untrust
      Index: 180
      Source addresses: s_ad1
      Destination addresses: d_ad1
      Applications
```

show security policy-report report-type scheduler

`user@host>` **show security policy-report report-type scheduler**

```
Logical system: root-logical-system
  Problem: Policy p2 has scheduler
     Policy: p2, Index: 129
     Source zone: trust
     Destination zone: untrust
     Source addresses: s_ad2
     Destination addresses: d_ad2
     Applications: app2
     Action: permit
     Scheduler: sch
```

show security policy-report report-type 1-year-not-hit

user@host> **show security policy-report report-type 1-year-not-hit**

```
Logical system: root-logical-system
  Problem: Not been hit for one year
  Recommendation: Please check if you need to remove policy p2
     Policy: p2, Index: 129
     Source zone: trust
     Destination zone: untrust
     Source addresses: s_ad2
     Destination addresses: d_ad2
     Applications: app2
     Action: permit
```

show security shadow-policies

Syntax

```
show security shadow-policies
<from-zone zone-name>
<global>
<logical-system logical-system-name>
<policy policy-name>
<reverse>
<root-logical-system>
<tenant tenant-name>
<to-zone zone-name>
```

Release Information

Command introduced in Junos OS Release 12.1X44-D10.
The **tenant** option is added in Junos OS Release 18.3R1.

Description

Displays the shadowing and shadowed policies in a policy list. The output displays the list of all policies that shadows other policies. The concept of policy shadowing refers to the situation where a policy higher in the policy list always takes effect before a subsequent policy. Because the policy lookup always uses the first policy it finds that matches the five-part tuple of the source and destination zone, source and destination address, and application type, if another policy applies to the same tuple (or a subset of the tuple), the policy lookup uses the first policy in the list and never reaches the second one. The existing show command for security shadow-policy is enhanced with tenant support.

Options

- **from-zone *zone-name***—Displays the name or ID of the source zone of the traffic.
- **global**—Displays the information about global policies.
- **logical-system**—Displays the name of the logical system.
- **policy**—Displays the shadow policy information for the given policy.
- **reverse**—Displays the policies which shadows the given policy.
- **root-logical-system**—Displays root logical system as default.
- **tenant**—Displays the name of the tenant system.
- **to-zone *zone-name***—Displays the shadow policy information for the given destination zone.

Required Privilege Level

view

RELATED DOCUMENTATION

show security policies | 524

List of Sample Output

show security shadow-policies from-zone zone-a to-zone zone-b on page 564
show security shadow-policies from-zone zone-a to-zone zone-b policy P1 on page 564
show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse on page 565
show security shadow-policies tenant TN1 from-zone trust to-zone untrust on page 565

Output Fields

Table 45 on page 564 lists the output fields for the **show security shadow-policies logical-system** command. Output fields are listed in the approximate order in which they appear.

Table 45: show security shadow-policies logical-system Output Fields

Field Name	Field Description
Policies	The policies shadowing one or more policies in the policy list.
Shadowed policies	The policies shadowed by one or more policies in the policy list.

Sample Output

show security shadow-policies from-zone zone-a to-zone zone-b

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b

    Policies              Shadowed policies
    P1                    P3
    P1                    P4
    P2                    P5
```

show security shadow-policies from-zone zone-a to-zone zone-b policy P1

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P1

   Policies              Shadowed policies
    P1                    P3
    P1                    P4
```

show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse

    Policies              Shadowed policies
     P1                    P4
```

show security shadow-policies tenant TN1 from-zone trust to-zone untrust

```
user@host> show security shadow-policies tenant TN1 from-zone trust to-zone untrust

Policies                  Shadowed policies
    p12                       p11
```

show security user-identification local-authentication-table

Syntax

```
show security user-identification local-authentication-table [ ( all [brief | extensive]) |ip-address ip-address | role
  role-name | start value | count value | user user-name]
```

Release Information

Command introduced in Junos OS Release 12.1.

Description

This command displays the content of the local authentication table by IP address.

all—(Optional) All entries displayed from the beginning of the table or from the specified starting entry.

brief—(Default) Uses a tabular format and truncates longer entries: username—displays up to 13 characters, roles—displays up to 32 characters.

extensive—(Optional) Displays the full names and all items.

count *value*—(Optional) The total number of entries to display.

ip-address *ip-address*—(Optional) The IP address of the entry to display.

role *role-name*—(Optional) The role name of the entries to display.

start *value*—(Optional) The first entry to display.

user *user-name*—(Optional) The username of the entry to display.

Required Privilege Level

view

RELATED DOCUMENTATION

request security user-identification local-authorization-table add | 495

Understanding the User Identification Table | 186

List of Sample Output

show security user-identification local-authentication-table all on page 567
show security user-identification local-authentication-table ip-address on page 567
show security user-identification local-authentication-table start on page 568

show security user-identification local-authentication-table role on page 568

Output Fields

Table 46 on page 567 lists the output fields for the **show security user-identification local-authentication-table** command. Output fields are listed in the approximate order in which they appear.

Table 46: show security user-identification local-authentication-table Output Fields

Field Name	Field Description
Total entries	The number of entries in the table.
IP address	IP address of the associated user. **NOTE:** Only one user can be associated with an IP address.
Username	User associated with the specified IP address.
Roles	A comma-separated list of all roles associated with this IP address and user.

Sample Output

show security user-identification local-authentication-table all

```
user@host> show security user-identification local-authentication-table all
```

```
Total entries: 3
Source IP       Username     Roles
192.0.2.1       user1        role1
203.0.113.2     user1        role2
198.51.100.3    user3        role1, role2
```

show security user-identification local-authentication-table ip-address

```
user@host> show security user-identification local-authentication-table ip-address 203.0.113.2
```

```
Ip-address: 203.0.113.2
    Username: user2
    Roles: role2, role3, role1
```

show security user-identification local-authentication-table start

```
user@host> show security user-identification local-authentication-table start 2 count 2
```

```
Total entries: 2
    Ip-address: 203.0.113.2
    Username: user2
    Roles: role2, role3, role1

    Ip-address: 198.51.100.3    Username: user3
    Roles: role2, role3
```

show security user-identification local-authentication-table role

```
user@host> show security user-identification local-authentication-table role qa3456
```

```
Total entries: 3
    Ip-address: 203.0.113.2
    Username: dev-grp-3
    Roles: qa432, qa3456, qa84, qa794

    Ip-address: 198.51.100.3
    Username: dev-qa
    Roles: qa3456, qa3985, qa23

    Ip-address: 203.0.113.2
    Username: brandall
    Roles: qa3456
```

show security user-identification role-provision all

Syntax

```
show security user-identification role-provision all
```

Release Information

Command introduced in Junos OS Release 12.1.

Description

Display all the available user roles for policy provisioning. The output combines user roles from all available UITs.

Required Privilege Level

view

RELATED DOCUMENTATION

show security user-identification user-provision all | 573

show security user-identification source-identity-provision all | 571

List of Sample Output

show security user-identification role-provision all on page 569

Output Fields

Table 47 on page 569 lists the output fields for the **show security user-identification role-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 47: show security user-identification role-provision all Output Fields

Field Name	Field Description
Roles	A comma-separated list of all user roles available for provisioning in user role policies. This list combines user roles from both the local authentication table and any UAC authentication tables that have been configured.

Sample Output

show security user-identification role-provision all

```
user@host> show security user-identification role-provision all
```

```
Roles: role1, role2, role3, role4, role_0_1, role_1_1
```

show security user-identification source-identity-provision all

Syntax

```
show security user-identification source-identity-provision all
```

Release Information

Command introduced in Junos OS Release 12.1X44-D10.

Description

Display the available source identities for policy provisioning. The output combines users and user roles from all available UITs.

Required Privilege Level

view

RELATED DOCUMENTATION

- show security user-identification role-provision all | 569
- show security user-identification user-provision all | 573

List of Sample Output

show security user-identification source-identity-provision all on page 572

Output Fields

Table 48 on page 571 lists the output fields for the **show security user-identification source-identity-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 48: show security user-identification source-identity-provision all Output Fields

Field Name	Field Description
Source identities	A comma-separated list of all users and user roles available for policy provisioning. This list combines users and user roles from both the local authentication table and any UAC authentication tables that have been configured.

Sample Output

show security user-identification source-identity-provision all

user@host> **show security user-identification source-identity-provision all**

```
Source identities: ariana, ben, guest5, role1, role2, role3, role4, role_0_1,
role_1_1,u1, user2
```

show security user-identification user-provision all

Syntax

```
show security user-identification user-provision all
```

Release Information

Command introduced in Release Junos OS 12.1X44-D10.

Description

Display the available user names for policy provisioning. The output combines users from all available UITs.

Required Privilege Level

view

RELATED DOCUMENTATION

show security user-identification role-provision all | 569

show security user-identification source-identity-provision all | 571

List of Sample Output

show security user-identification user-provision all on page 573

Output Fields

Table 49 on page 573 lists the output fields for the **show security user-identification user-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 49: show security user-identification user-provision all Output Fields

Field Name	Field Description
Users	A comma-separated list of all users available for policy provisioning. This list combines users from both the local authentication table and any UAC authentication tables that have been configured.

Sample Output

show security user-identification user-provision all

```
user@host> show security user-identification user-provision all
```

```
Users: ariana, ben, guest5, u1 user2, ...
```

show security zones

Syntax

```
show security zones
<zone-name>
<all-logical-systems-tenants>
<detail>
<logical-system (logical-system-name | all)>
<root-logical-system>
<tenant (tenant-name | all)>
<terse>
<type (functional | security)>
```

Release Information

Command introduced in Junos OS Release 8.5.
tenant option introduced in Junos OS Release 18.3R1.

Description

Displays the information about the security zones. You can define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.

Options

- ***none***—Displays information about all the security zones configured.
- ***zone-name***—(Optional) Displays information about the specified security zone.
- **all-logical-systems-tenants**—(Optional) Displays the information about the security zone of all logical systems and tenant systems.
- **detail**—(Optional) Displays the detail level information about the security zone.
- **logical-system *logical-system-name***—(Optional) Displays the information about the security zones of a specified logical system.
- **logical-system all**—(Optional) Displays the information about the security zones of all logical systems.
- **root-logical-system**—(Optional) Displays the information about the security zones of the root logical system.
- **tenant *tenant-name***—(Optional) Displays the information about the security zones of a specified tenant system.
- **tenant all**—(Optional) Displays the information about the security zones of all tenant systems.
- **terse**—(Optional) Displays the specified level information about the security zone.

- **type functional**—(Optional) Displays the information for functional zones.
- **type security**—(Optional) Displays the information for security zones.

Required Privilege Level
view

RELATED DOCUMENTATION

Security Zones Overview | 27
Supported System Services for Host Inbound Traffic | 32
security-zone | 418

List of Sample Output
show security zones on page 577
show security zones abc on page 578
show security zones all-logical-systems-tenants on page 578
show security zones abc detail on page 579
show security zones logical-system LSYS1 on page 580
show security zones logical-system all on page 580
show security zones root-logical-system on page 580
show security zones tenant TSYS1 on page 581
show security zone tenant all on page 581
show security zones terse on page 582
show security zones type security on page 582

Output Fields
Table 50 on page 576 lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

Table 50: show security zones Output Fields

Field Name	Field Description	Level of Output
Functional zone	Name of the functional zone.	none
Security zone	Name of the security zone.	detail none
Description	Description of the security zone.	detail none

Table 50: show security zones Output Fields *(continued)*

Field Name	Field Description	Level of Output
Policy configurable	Whether the policy can be configured or not.	detail none
Interfaces bound	Number of interfaces in the zone.	detail none
Interfaces	List of the interfaces in the zone.	detail none
Zone	Name of the zone.	terse
Type	Type of the zone.	terse
Logical system	Name of the logical system.	detail
Tenant	Name of the tenant system.	detail

Sample Output

show security zones

`user@host>` **show security zones**

```
Functional zone: management
   Description: This is the management zone.
   Policy configurable: No
   Interfaces bound: 1
   Interfaces:
     ge-0/0/0.0
Security zone: Host
   Description: This is the host zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     fxp0.0
Security zone: abc
```

```
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
Security zone: def
   Description: This is the def zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/2.0
```

show security zones abc

user@host> **show security zones abc**

```
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

show security zones all-logical-systems-tenants

user@host> **show security zones all-logical-systems-tenants**

```
Logical system: root-logical-system

Security zone: HOST
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: all
  Interfaces:

Security zone: junos-host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
```

```
  Interfaces:

Logical system: LSYS1

Security zone: z1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Logical system: TSYS1

Security zone: z3a
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Security zone: z3b
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Security zone: z3c
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zones abc detail

user@host> **show security zones abc detail**

```
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

show security zones logical-system LSYS1

```
user@host> show security zones logical-system LSYS1
```

```
Security zone: z1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zones logical-system all

```
user@host> show security zones logical-system all
```

```
Logical system: root-logical-system

Security zone: HOST
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: all
  Interfaces:

Security zone: junos-host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Logical system: LSYS1

Security zone: z1
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zones root-logical-system

```
user@host> show security zones root-logical-system
```

```
Security zone: HOST
```

```
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: all
  Interfaces:

Security zone: junos-host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zones tenant TSYS1

user@host> **show security zones tenant TSYS1**

```
Security zone: z3a
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Security zone: z3b
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

Security zone: z3c
 Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zone tenant all

user@host> **show security zone tenant all**

```
  Tenant: TSYS1


  Security zone: Host
```

```
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:

  Security zone: abc
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:xe-0/0/1.0

  Security zone: def
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:xe-0/0/3.0
```

show security zones terse

user@host> **show security zones terse**

```
Zone                    Type
my-internal             Security
my-external             Security
dmz                     Security
```

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: all
  Interfaces:

Security zone: junos-host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show security zones type

Syntax

```
show security zones type
(functional | security)
<detail | terse>
```

Release Information

Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.

Description

Display information about security zones of the specified type.

Options

- **functional**—Display functional zones.
- **security**—Display security zones.
- **detail** | **terse**—(Optional) Display the specified level of output.

Required Privilege Level

view

RELATED DOCUMENTATION

Security Zones Overview | 27

Supported System Services for Host Inbound Traffic | 32

security-zone | 418

List of Sample Output

show security zones type functional on page 584

show security zones type security on page 585

show security zones type security terse on page 585

show security zones type security detail on page 586

Output Fields

Table 51 on page 584 lists the output fields for the **show security zones type** command. Output fields are listed in the approximate order in which they appear.

Table 51: show security zones type Output Fields

Field Name	Field Description	Level of Output
Security zone	Zone name.	All levels
Description	Description of the security zone.	none detail
Policy configurable	Whether the policy can be configured or not.	none detail
Interfaces bound	Number of interfaces in the zone.	none detail
Interfaces	List of the interfaces in the zone.	none detail
Zone	Name of the zone.	All levels
Type	Type of the zone.	All levels

Sample Output

show security zones type functional

`user@host>` **show security zones type functional**

```
Functional zone: management
  Description: management zone
  Policy configurable: No
  Interfaces bound: 0
  Interfaces:
```

Sample Output

show security zones type security

user@host> **show security zones type security**

```
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

Sample Output

show security zones type security terse

user@host> **show security zones type security terse**

```
Zone                    Type
trust                   Security
untrust                 Security
junos-host              Security
```

Sample Output

show security zones type security detail

user@host> **show security zones type security detail**

```
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

show system services dns dns-proxy

Syntax

```
show system services dns dns-proxy
```

Release Information

Command introduced in Junos OS Release 12.1X44-D10.

Description

Display domain name system (DNS) proxy information. This option is supported on the SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices.

Options

- **none**—Display DNS proxy statistics information.
- **cache**—(Optional) Display the DNS proxy cache.
- **statistics**—(Optional) Display the DNS proxy statistics.

Required Privilege Level

view

RELATED DOCUMENTATION

clear system services dns dns-proxy | 489

dns-proxy | 324

List of Sample Output

show system services dns-proxy statistics on page 588
show system services dns-proxy cache on page 589
show system services dns-proxy cache <viewname V1> on page 589

Output Fields

Table 52 on page 588 lists the output fields for the **show system services dns-proxy** command. Output fields are listed in the approximate order in which they appear.

Table 52: show system services dns-proxy

Field Name	Field Description
DNS proxy statistics	Display information about the DNS proxy. • **Status**—State of the proxy server as Enabled or disabled. • **Queries received**—Number of DNS queries received by the DNS proxy. • **Responses sent**—Number of DNS responses sent by the DNS proxy. • **Queries forwarded**—Number of DNS queries forwarded by the DNS proxy. • **Negative responses**—Number of negative responses the DNS proxy sent to the DNS client. • **Retry requests**—Number of retries the DNS proxy received from the DNS client. • **Pending requests**—Number of pending queries the DNS proxy has yet to send the DNS client a response for. • **Server failures**—Number of DNS proxy server failures.
Hostname	Hostname of the host that has been cached.
IP address	IP address of the host.
Time-to-live	Length of time before an entry is purged from the DNS cache.
Type	Type of DNS Resource Record. For example, A records refer to IPv4 host addresses.
Class	Class of DNS. A parameter used to define a DNS Resource Record. For example, IN class is used for Internet domain names.

Sample Output

show system services dns-proxy statistics

`user@host>` **show system services dns-proxy statistics**

```
DNS proxy statistics       :
    DNS proxy statistics    :
    Status              : enabled
    IPV4 Queries received   : 30
    IPV6 Queries received   : 0
    Responses sent      : 30
```

```
    Queries forwarded   : 13
    Negative responses  : 23
    Positive responses  : 23
    Retry requests      : 0
    Pending requests    : 0
    Server failures     : 0
    Interfaces          : fe-0/0/0.0, fe-1/0/1.0
```

show system services dns-proxy cache

user@host>**show system services dns-proxy cache**

```
Hostname                Time-to-live      Type        Class   IP address/Hostname
device1.example.com        408               A           IN      207.17.137.229
device2.example.com        408               A           IN      192.0.2.50
device3.example.com        408               A           IN      192.0.2.11
device4.example.com        408               A           IN      10.209.194.131
device5.example.com        408               A           IN      10.10.4.202
device6.example.com        408               A           IN      10.16.0.11
device7.example.com        408               A           IN      192.0.2.100
a.l.example.com            408               A           IN      203.0.113.9
b.l.example.com            408               A           IN      198.51.100.9
maps.l.example.com         408               A           IN      198.51.100.104
c.l.example.com            408               A           IN      198.51.100.91
d.l.example.com            408               A           IN      198.51.100.89
e.l.example.com            408               A           IN      198.51.100.39
g.l.example.com            408               A           IN      198.51.100.69
device8.example.com.       408               A           IN      192.0.2.123
mail.example.com.          408               CNAME       IN
device8.example.com.
```

show system services dns-proxy cache <viewname V1>

user@host>**show system services dns-proxy cache <viewname V1>**

```
Hostname                Time-to-live    Type        Class    IP address/Hostname
device1.example.com.       495            A           IN       198.51.100.123
mail.example.com.          495           CNAME       IN       device1.example.com.
```

show system services dynamic-dns

Syntax

```
show system services dynamic-dns
```

Release Information

Command introduced in Junos OS Release 12.1X44-D10.

Description

Display information about dynamic DNS clients. This option is supported on the SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices.

Required Privilege Level

view

RELATED DOCUMENTATION

dynamic-dns | 330

List of Sample Output

show system services dynamic-dns client on page 591
show system services dynamic-dns client detail on page 591

Output Fields

Table 53 on page 590 lists the output fields for the **show system services dynamic-dns** command. Output fields are listed in the approximate order in which they appear.

Table 53: show system services dynamic-dns

Field Name	Field Description
Hostname	Hostname of the registered client
Server	DDNS server name
Agent	Name of the DDNS agent
Last response	Status of the last response
Last update	Date and time of the last update
Interface	Name of the interface

Sample Output

show system services dynamic-dns client

user@host> **show system services dynamic-dns client**

```
Internal hostname      Server                  Last response
device1.example.com         example.org                success
device2.example.com.        example.org                failure
```

show system services dynamic-dns client detail

user@host>**show system services dynamic-dns client detail**

```
Hostname     : device1.example.com
Server       : example.org
Agent        : branch-0.1
Last response: success
Last update  : 2006-08-29 04:02:52 PDT
Interface    : fe-0/0/0.0

Hostname     : device2.example.com
Server       : example.org
Agent        : Branch-0.1
Last response: failure
Last update  : 2006-08-29 04:03:03 PDT
Interface    : fe-0/0/0.0
```