JUNIPER NETWORKS

Junos® OS

User Logical System Administrator Feature Guide for Security Devices

Release
12.1X46-D10

Published: 2013-11-15

Copyright © 2013, Juniper Networks, Inc.

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

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

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

Junos® OS User Logical System Administrator Feature Guide for Security Devices
12.1X46-D10
Copyright © 2013, 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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

Part 4 Index

Copyright © 2013, Juniper Networks, Inc.

List of Figures

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

List of Tables

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

About the Documentation

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- SRX1400
- SRX3400
- SRX3600
- SRX5600
- SRX5800
- SRX5400

Copyright © 2013, Juniper Networks, Inc.

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
   ```


Copyright © 2013, Juniper Networks, Inc.

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 the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii 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.

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

Copyright © 2013, Juniper Networks, Inc.

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*
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

Copyright © 2013, Juniper Networks, Inc.

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/

Copyright © 2013, Juniper Networks, Inc.

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

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

Opening a Case with JTAC

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

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

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

Copyright © 2013, Juniper Networks, Inc.

PART 1

Overview

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 1

Logical Systems

Understanding Logical Systems for SRX Series Services Gateways

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

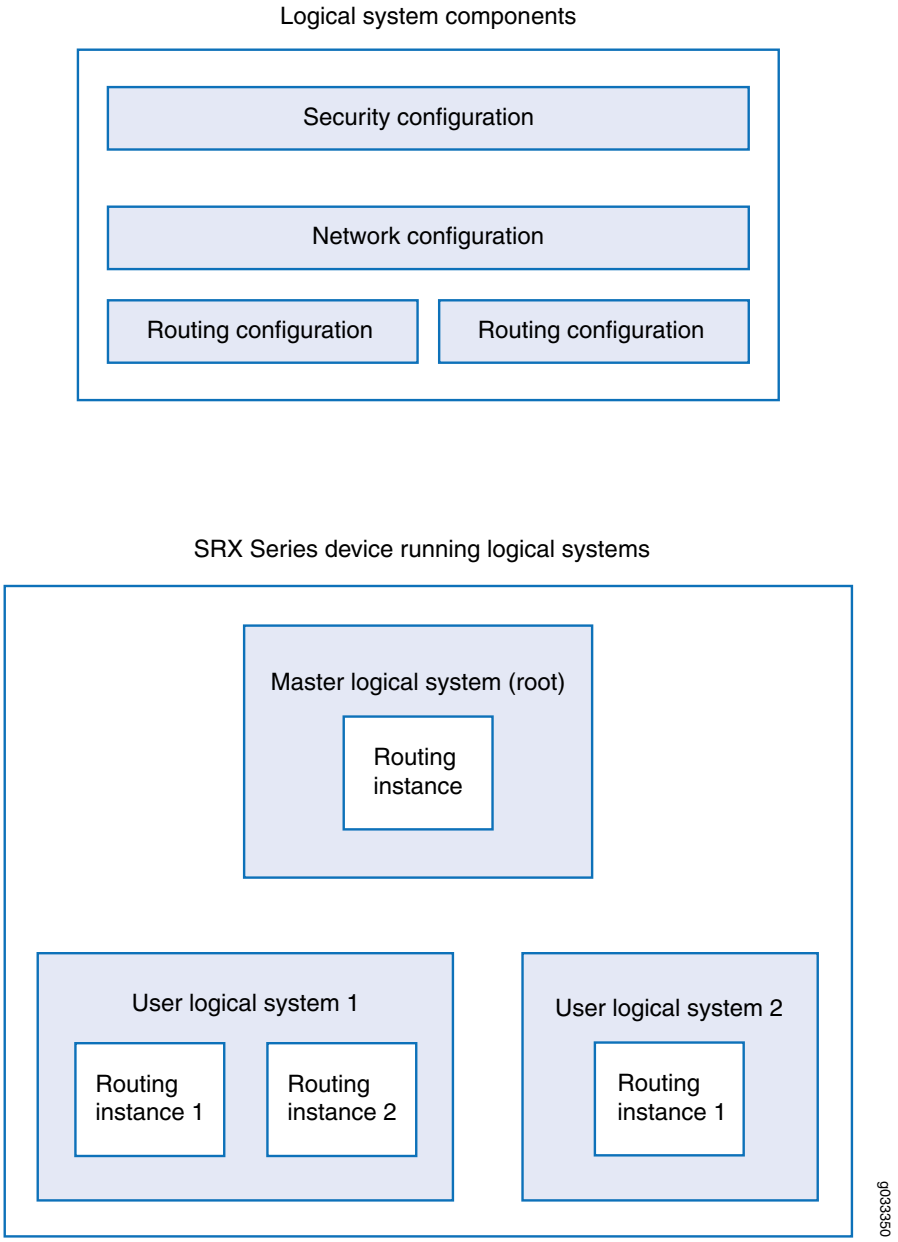
Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming an SRX Series device into a multitenant logical systems device, you can give various departments, organizations, customers, and partners–depending on your environment–private use of portions of its resources and a private view of the device. Using logical systems, you can share system and underlying physical machine resources among discrete user logical systems and the master logical system.

The logical systems feature runs with the Junos operating system (Junos OS) on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

The top part of Figure 1 on page 4 shows the three main configuration components of a logical system. The lower part of the figure shows a single device with a master logical system and discrete user logical systems.

Copyright © 2013, Juniper Networks, Inc.

Figure 1: Understanding Logical Systems



Logical systems on SRX Series devices offer many benefits, allowing you to:

- Curtail costs. Using logical systems, you can reduce the number of physical devices required for your company. Because you can consolidate services for various groups of users on a single device, you reduce both hardware costs and power expenditure.
- Create many logical systems on a single device and provision resources and services for them quickly. Because services are converged, it is easier for the master, or root, administrator to manage a single device configured for logical systems than it is to manage many discrete devices.

Copyright © 2013, Juniper Networks, Inc.

You can deploy an SRX Series device running logical systems in many environments, in particular, in the enterprise and in the data center.

- In the enterprise, you can create and provision logical systems for various departments and groups.

  You can configure logical systems to enable communication among groups sharing the device. When you create logical systems for various departments on the same device, users can communicate with one another without traffic leaving the device if you have configured an interconnect logical system to serve as an internal switch. For example, members of the product design group, the marketing department, and the accounting department sharing an SRX Series Services Gateway running logical systems can communicate with one another just as they could if separate devices were deployed for their departments. You can configure logical systems to interconnect through *logical tunnel (lt-0/0/0)* internal interfaces. The lt-0/0/0 interfaces on the interconnect logical system connect to an lt-0/0/0 interface that you configure for each logical system. The interconnect logical system switches traffic between logical systems. The SRX Series device running logical systems provides for high, fast interaction among all logical systems created on the device when an interconnect logical system is used.

  Logical systems on the same device can also communicate with one another directly through ports on the device, as if they were separate devices. Although this method allows for direct connections between logical systems, it consumes more resources—you must configure interfaces and an external switch—and therefore it is more costly.

- In the data center, as a service provider, you can deploy an SRX Series device running logical systems to offer your customers secure and private user logical systems and discrete use of the device's resources.

  For example, one corporation might require 10 user logical systems and another might require 20. Because logical systems are secure, private, and self-contained, data belonging to one logical system cannot be viewed by administrators or users of other logical systems. That is, employees of one corporation cannot view the logical systems of another corporation.

Logical systems include both master and user logical systems and their administrators. The roles and responsibilities of the master administrator and those of a user logical system administrator differ greatly. This differentiation of privileges and responsibilities is considered role-based administration and control.

NOTE: **To use the internal switch, which is optional, you must also configure an interconnect logical system. The interconnect logical system does not require an administrator.**

Related Documentation

- Understanding the Master Logical System and the Master Administrator Role on page 17
- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Understanding the Fundamentals and Constraints of Logical Systems

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This topic covers basic information about logical systems features and limitations.

- By default, logical systems delivers a master logical system, which exists at the root level. You can purchase licenses for logical systems that you intend to create with the total not exceeding 32.
- You can configure up to 32 security profiles.
- You can configure one or more master administrators to oversee administration of the device and the logical systems they configure.

  As master administrator for an SRX Series Services Gateway running logical systems, you have root control over the device, its resources, and the logical systems that you create. You allocate security, networking, and routing resources to user logical systems. You can configure one logical system to serve as an interconnect logical system virtual private LAN service (VPLS) switch. The interconnect logical system, which is not mandatory, does not require security resources. However, if you configure an interconnect logical system, you must bind a dummy security profile to it. The master administrator configures it and all lt-0/0/0 interfaces for it.
- A user logical system can have one or more administrators, referred to as user logical system administrators. The master administrator creates login accounts for these administrators and assigns them to a user logical system. Currently, the master administrator must configure all user logical system administrators. The first assigned user logical administrator cannot configure additional user logical system administrators for his logical system. As a user logical system administrator, you can configure the resources assigned to your user logical system, including logical interfaces assigned by the master administrator, routing instances and their routes, and security components. You can display configuration information only for your logical system.
- A logical system can include more than one routing instance based on available system resources.
- You cannot configure class of service on lt-0/0/0 interfaces.
- The trace and debug features are supported at the root level only.
- Commit rollback is supported at the root level only.
- The master administrator can configure Application Layer Gateways (ALGs) at the root level. The configuration is inherited by all user logical systems. It cannot be configured discretely for user logical systems.
- The master administrator can configure IDP policies at the root level and then apply an IDP policy to a user logical system.
- Only the master administrator can create user accounts and login IDs for users for all logical systems. The master administrator creates these user accounts at the root level and assigns them to the appropriate user logical systems.

Copyright © 2013, Juniper Networks, Inc.

- The same name cannot be used in two separate logical systems. For example, if logical-system1 includes a user with Bob configured as the username, then other logical systems on the device cannot include a user with the username Bob.
- Configuration for users for all logical systems and all user logical systems administrators must be performed at the root level by the master administrator.

Related Documentation

- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding the Master Logical System and the Master Administrator Role on page 17
- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- *Junos OS Logical Systems Library for Security Devices*

Understanding Licenses for Logical Systems on SRX Series Devices

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This topic provides licensing information for SRX Series devices running logical systems. For general licensing information, such as how to install a license, see the *Installation and Upgrade Guide for Security Devices*.

By default, a device running logical systems delivers a master logical system at the root level. You can purchase licenses for other logical systems that you intend to create. If you intend to configure an interconnect logical system to use as a switch, it also requires a license.

Complications arise if the number of logical systems that you configure exceeds the number of licenses that you have purchased. The system will allow you to configure additional logical systems. However, when you attempt to commit their configurations, the system issues a warning message similar to the following: **Warning: 2 more license(s) are needed, logical system won't work without license!**. The message indicates the number of logical systems without licenses. We recommend that you do not configure more logical systems than the number of licenses you have purchased.

If you configure more logical systems than the number of licenses that you have purchased, the additional logical systems will not be activated until a license is available. The system will drop packets destined to them. They are inactive.

When a logical system is deleted, its license is freed up. That license is assigned to an inactive logical system, and the logical system is activated.

You can use the **show system license status logical-system all** command on the command-line interface (CLI) to determine which logical systems are active.

```
user@host>  show system license status logical-system all
logical system name      license status
root-logical-system      enabled
LSYS2              enabled
```

Copyright © 2013, Juniper Networks, Inc.

```
LSYS0              enabled
LSYS11             enabled
LSYS12             enabled
LSYS23             enabled
LSYS10             enabled
LSYS13             enabled
LSYS18             enabled
```

When you use SRX Series devices running logical systems in a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Related Documentation

- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding the Master Logical System and the Master Administrator Role on page 17
- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- *Junos OS Logical Systems Library for Security Devices*

Understanding the Interconnect Logical System and Logical Tunnel Interfaces

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This topic covers the interconnect logical system that serves as an internal virtual private LAN service (VPLS) switch connecting one logical system on the device to another. The topic also explains how logical tunnel (lt-0/0/0) interfaces are used to connect logical systems through the interconnect logical system.

A device running logical systems can use an internal VPLS switch to pass traffic without it leaving the device. The interconnect logical system switches traffic across logical systems that use it. Although a virtual switch is used typically, it is not mandatory. If you choose to use a virtual switch, you must configure the interconnect logical system. There can be only one interconnect logical system on a device.

For communication between logical systems on the device to occur, you must configure an lt-0/0/0 interface on each logical system that will use the internal switch, and you must associate it with its peer lt-0/0/0 interface on the interconnect logical system, effectively creating a logical tunnel between them. You define a peer relationship at each end of the tunnel when you configure the logical system's lt-0/0/0 interfaces.

You might want all logical systems on the device to be able to communicate with one another without using an external switch. Alternatively, you might want some logical systems to connect across the internal switch but not all of them.

The interconnect logical system does not require security resources assigned to it through a security profile. However, you must assign a dummy security profile containing no

Copyright © 2013, Juniper Networks, Inc.

resources to the interconnect logical system. Otherwise you will not be able to successfully commit the configuration for it.

WARNING: **If you configure an lt-0/0/0 interface in any user logical system or the master logical system and you do not configure an interconnect logical system containing a peer lt-0/0/0 interface for it, the commit will fail.**

An SRX Series device running logical systems can be used in a chassis cluster. Each node has the same configuration, including the interconnect logical system.

When you use SRX Series devices running logical systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Related Documentation

- *Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems*
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding Logical Systems in the Context of Chassis Cluster on page 37
- *Junos OS Logical Systems Library for Security Devices*

Understanding Flow in Logical Systems for SRX Series Devices

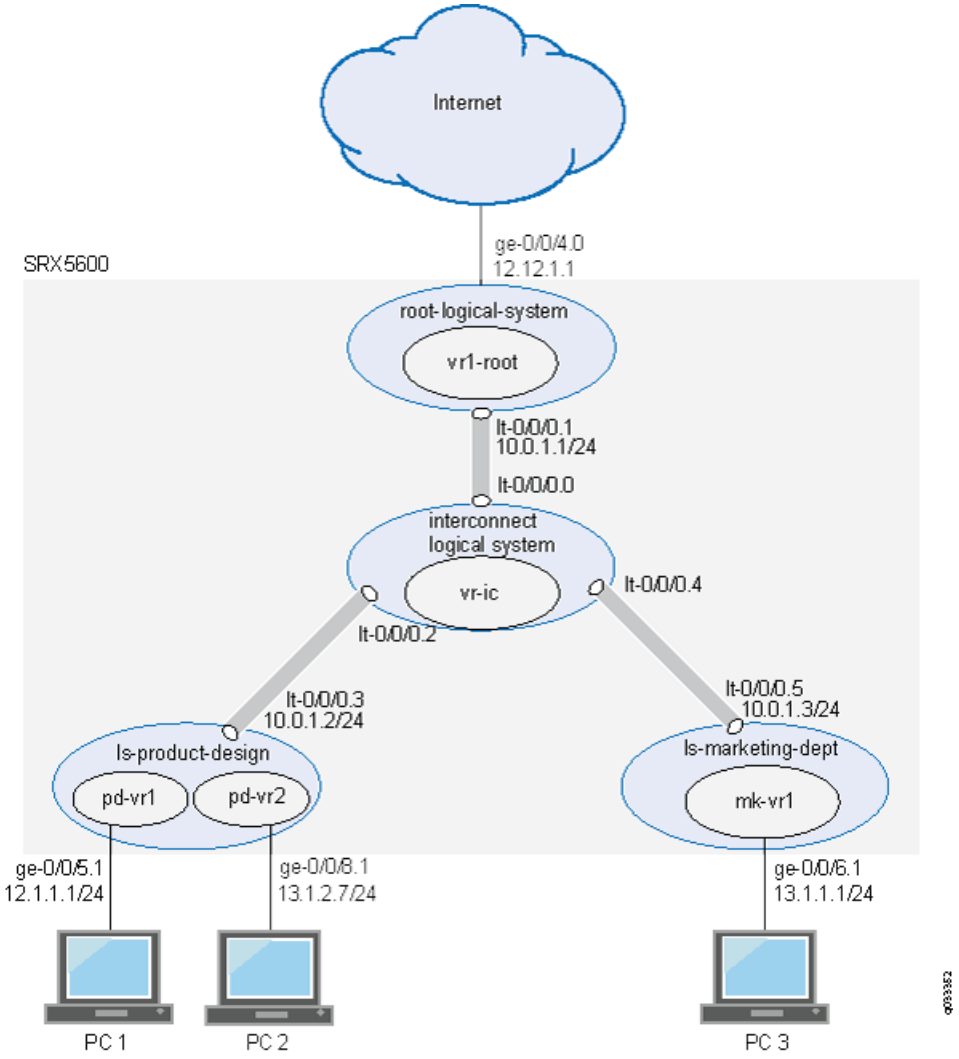
Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This topic explains how packets are processed in flow sessions on SRX Series devices running logical systems. It describes how an SRX Series device running logical systems handles pass-through traffic in a single logical system and between logical systems. It also covers self-traffic as self-initiated traffic within a logical system and self-traffic terminated on another logical system. Before addressing logical systems, the topic provides basic information about the SRX Series architecture in with respect to packet processing and sessions. Finally, it addresses sessions and how to change session characteristics.

The concepts explained in this example rely on the topology shown in Figure 2 on page 10.

Copyright © 2013, Juniper Networks, Inc.

Figure 2: Logical Systems, Their Virtual Routers, and Their Interfaces



- Understanding Junos OS SRX Series Services Gateways Architecture on page 11
- Session Creation for Devices Running Logical Systems on page 11
- Understanding Flow on Logical Systems on page 12
- Understanding Packet Classification on page 12
- Handling Pass-Through Traffic for Logical Systems on page 13
- Handling Self-Traffic on page 14
- Understanding Session and Gate Limitation Control on page 16
- Understanding Sessions on page 16
- About Configuring Sessions on page 16

Copyright © 2013, Juniper Networks, Inc.

Understanding Junos OS SRX Series Services Gateways Architecture

Junos OS for the SRX5600 and SRX5800 devices is a distributed parallel processing high-throughput, high-performance system. The distributed parallel processing architecture includes multiple processors to manage sessions, run security and perform other services processing.

The SRX5600 and SRX5800 Services Gateways include I/O cards (IOCs) and Services Processing Cards (SPCs) that each contain processing units that process a packet as it traverses the device. A Network Processing Unit (NPU) runs on an IOC. An IOC has one or more NPUs. One or more Services Processing Units (SPUs) run on an SPC.

The processing units have different functions. For example:

- An NPU processes packets discretely. It performs sanity checks and applies some screens that are configured for the interface, such as denial-of-service (DoS) screens, to the packet.
- An SPU manages the session for the packet flow and applies security features and other services to the packet. It also applies packet-based stateless firewall filters, classifiers, and traffic shapers to the packet.
- The system uses one processor as a central point to take care of arbitration and allocation of resources and distribute sessions. The CP assigns an SPU to be used for a particular session when the first packet of its flow is processed.

These discrete, cooperating parts of the system each store the information identifying whether a session exists for a stream of packets and the information against which a packet is matched to determine whether it belongs to an existing session. This architecture allows the device to distribute processing of all sessions across multiple SPUs.

An SPU processes the packets of a flow according to the security features and other services configured for the session. It also allows an NPU to determine whether a session exists for a packet, to check the packet, and to apply screens to it.

Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that are established for the first packet of the packet stream when the flow session is established. Most packet processing occurs within a flow. For the distributed processing architecture of the services gateway, some packet-based processing, such as traffic shaping, occurs on the NPU. Some packet-based processing, such as application of classifiers to a packet, occurs on the SPU.

Configuration settings that determine the fate of a packet—such as the security policy that applies to it, Aplication Layer Gateway (ALG)s configured for it, if NAT should be applied to translate the packet's source and/or destination IP address—are assessed for the first packet of a flow.

Session Creation for Devices Running Logical Systems

Session establishment for SRX Series devices running logical systems differs in minor ways from that of SRX series devices not running logical systems. Despite the complexities that logical systems introduce, traffic is handled in a manner similar to how it is handled

Copyright © 2013, Juniper Networks, Inc.

on SRX Series devices not running logical systems. Flow-based packet processing, which is stateful, requires the creation of sessions. In considering flow based processing and session establishment for logical systems, it helps to think of each logical system on the device as a discrete device with respect to session establishment.

A session is created, based on routing and other classification information, to store information and allocate resources for a flow. Basically, a session is established when traffic enters a logical system interface, route lookup is performed to identify the next hop interface, and policy lookup is performed.

Optionally, logical systems enable you to configure an internal software switch. This virtual private LAN switch (VPLS) is implemented as an interconnect logical system. It enables both transit traffic and traffic terminated at a logical system to pass between logical systems. To enable traffic to pass between logical systems, logical tunnel (lt-0/0/0) interfaces across the interconnect logical system are used.

Communication between logical systems across the interconnect logical system requires establishment of two sessions: one for traffic that enters a logical system and exits its lt-0/0/0 interface, and one for traffic that enters the lt-0/0/0 interface of another logical system and either exits the device through one of its physical interface or is destined for it.

NOTE: **Packet sequence occurs at the ingress and the egress interfaces. Packets traveling between logical systems might not be processed in the order in which they were received on the physical interface.**

Understanding Flow on Logical Systems

To understand how traffic is handled for logical systems, it is helpful to consider each logical system as a discrete device.

NOTE: **Traffic is processed for the master logical system in the same way as it is for user logical systems on the device.**

Understanding Packet Classification

Packet classification is assessed the same way for SRX Series devices running with or without logical systems. Filters and class-of-service features are typically associated with an interface to influence which packets are allowed to transit the system and to apply special actions to packets as needed. (Within a flow, some packet-based processing also takes place on an SPU.)

Packet classification is based on the incoming interface and performed at the ingress point. Traffic for a dedicated interface is classified to the logical system that contains that interface. Within the context of a flow, packet classification is based on both the physical interface and the logical interface.

Copyright © 2013, Juniper Networks, Inc.

Handling Pass-Through Traffic for Logical Systems

For SRX Series devices not running logical systems, pass-through traffic is traffic that enters and exits a device. You can think of pass-through traffic for logical systems similarly, but as having a larger dimension as a result of the nature of a multitenant device. For SRX Series devices running logical systems, pass-through traffic can exist within a logical system or between logical systems.

Pass-Through Traffic Within a Logical System

For pass-through traffic within a logical system, traffic comes in on an interface belonging to one of the logical system's virtual routing instances, and it is sent to another of its virtual routing instances. To exit the device, the traffic is sent out an interface belonging to the second virtual routing instance. The traffic does not transit between logical systems but rather enters and exits the device in a single logical system. Pass-through traffic within a logical system is transmitted according to the routing tables in each of its routing instances.

Consider how pass-through traffic is handled within a logical system given the topology shown in Figure 2 on page 10.

- When a packet arrives on interface ge-0/0/5, it is identified as belonging to the ls-product-design logical system.
- Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1 with pd-vr2 identified as the next hop.
- A second route lookup is performed in pd-vr2 to identify the egress interface to use—in this case— ge-0/0/8.
- The packet is sent out ge-0/0/8 to the network.
- The security policy lookup is performed in ls-product-design, and one session is established.

Pass-Through Traffic Between Logical Systems

Pass-through traffic between logical systems is complicated by fact that each logical system has an ingress and an egress interface that the traffic must transit. It is as if traffic were coming into and going out from two devices.

Two sessions must be established for pass-through traffic between logical systems. (Note that policy lookup is performed in both logical systems).

- On the incoming logical system, one session is set up between the ingress interface (a physical interface) and its egress interface (an lt-0/0/0 interface).
- On the egress logical system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second logical system) and its egress interface (a physical interface).

Copyright © 2013, Juniper Networks, Inc.

Consider how pass-through traffic is handled across logical systems in the topology shown in Figure 2 on page 10.

- A session is established in the incoming logical system.
  - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the ls-product-design logical system.
  - Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1.
  - As a result of the lookup, the egress interface for the packet is identified as lt-0/0/0.3 with the next hop identified as lt-0/0/0.5, which is the ingress interface in the ls-marketing-dept.
  - A session is established between ge-0/0/5 and lt-0/0/0.3.
- A session is established in the outgoing logical system.
  - The packet is injected into the flow again from lt-0/0/0.5, and the logical system context identified as ls-marketing-dept is derived from the interface.
  - Packet processing continues in the ls-marketing-dept logical system.
  - To identify the egress interface, route lookup for the packet is performed in the mk-vr1 routing instances.
  - The outgoing interface is identified as ge-0/0/6, and the packet is transmitted from the interface to the network.

Handling Self-Traffic

Self-traffic is traffic that originates in a logical system on the device and is either sent out to the network from that logical system or is terminated on another logical system on the device.

Self-Initiated Traffic

Self-initiated traffic is generated from a source logical system context and forwarded directly to the network from the logical system interface.

The following process occurs:

- When a packet is generated in a logical system, a process for handling the traffic is started in the logical system.
- Route lookup is performed to identify the egress interface, and a session is established.
- The logical system performs a policy lookup and processes the traffic accordingly.
- If required, a management session is set up.

Consider how self-initiated traffic is handled across logical systems given the topology shown in Figure 2 on page 10.

 Copyright © 2013, Juniper Networks, Inc.

- A packet is generated in the ls-product-design logical system, and a process for handling the traffic is started in the logical system.
- Route lookup performed in pd-vr2 to identifies the egress interface as ge-0/0/8.
- A session is established.
- The packet is transmitted to the network from ge-0/0/8.

Traffic Terminated on a Logical System

When a packet enters the device on an interface belonging to a logical system and the packet is destined for another logical system on the device, the packet is forwarded between the logical systems in the same manner as is pass-through traffic. However, route lookup in the second logical system identifies the local egress interface as the packet destination. Consequently the packet is terminated on the second logical system as self-traffic.

- For terminated self-traffic, two policy lookups are performed, and two sessions are established.
  - On the incoming logical system, one session is set up between the ingress interface (a physical interface) and its egress interface (an lt-0/0/0 interface).
  - On the destination logical system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second logical system) and the local interface.

Consider how terminated self-traffic is handled across logical systems in the topology shown in Figure 2 on page 10.

- A session is established in the incoming logical system.
  - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the ls-product-design logical system.
  - Because ge-0/0/5 belongs to the pd-vr1 routing instance, route lookup is performed in pd-vr1.
  - As a result of the lookup, the egress interface for the packet is identified as lt-0/0/0.3 with the next hop identified as lt-0/0/0.5, the ingress interface in the ls-marketing-dept.
  - A session is established between ge-0/0/5 and lt-0/0/0.3.
- A management session is established in the destination logical system.
  - The packet is injected into the flow again from lt-0/0/0.5, and the logical system context identified as ls-marketing-dept is derived from the interface.
  - Packet processing continues in the ls-marketing-dept logical system.
  - Route lookup for the packet is performed in the mk-vr1 routing instance. The packet is terminated in the destination logical system as self-traffic.
  - A management session is established.

Copyright © 2013, Juniper Networks, Inc.

Understanding Session and Gate Limitation Control

The logical systems flow module provides session and gate limitation to ensure that these resources are shared fairly among the logical systems. Resources allocation and limitations for each logical system are specified in the security profile bound to the logical system.

- For session limiting, the system checks the first packet of a session against the maximum number of sessions configured for the logical system. If the maximum is reached, the device drops the packet and logs the event.
- For gate limiting, the device checks the first packet of a session against the maximum number of gates configured for the logical system. If the maximum number of gates for a logical system is reached, the device rejects the gate open request and logs the event.

Understanding Sessions

Sessions are created based on routing and other classification information to store information and allocate resources for a flow. You can change some characteristics of sessions, such as when a session is terminated. For example, you might want to ensure that a session table is never entirely full to protect against an attacker's attempt to flood the table and thereby prevent legitimate users from starting sessions.

About Configuring Sessions

Depending on the protocol and service, a session is programmed with a timeout value. For example, the default timeout for TCP is 1800 seconds. The default timeout for UDP is 60 seconds. When a flow is terminated, it is marked as invalid, and its timeout is reduced to 10 seconds. If no traffic uses the If no traffic uses the session before the service timeout, the session is aged out and freed to a common resource pool for reuse.

You can affect the life of a session in the following ways:

- Age out sessions, based on how full the session table is.
- Set an explicit timeout for aging out TCP sessions.
- Configure a TCP session to be invalidated when it receives a TCP RST (reset) message.
- You can configure sessions to accommodate other systems as follows:
  - Disable TCP packet security checks.
  - Change the maximum segment size.

Related Documentation

- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 8
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 2

Roles

Understanding the Master Logical System and the Master Administrator Role

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

When, as a master administrator, you initialize an SRX Series device running logical systems, a master logical system is created at the root level. You can log in to the device as root and change the root password.

By default, all system resources are assigned to the master logical system, and the master administrator allocates them to the user logical systems.

As master administrator, you manage the device and all its logical systems. You also manage the master logical system and configure its assigned resources. There can be more than one master administrator managing a device running logical systems.

- The master administrator's role and main responsibilities include:
  - Creating user logical systems and configuring their administrators. You can create one or more user logical system administrators for each user logical system.
  - Creating login accounts for users for all logical systems and assigning them to the appropriate logical systems.
  - Configuring an interconnect logical system if you want to allow communication between logical systems on the device. The interconnect logical system acts as an internal switch. It does not require an administrator.

    To configure an interconnect logical system, you configure lt-0/0/0 interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for establishment of tunnels.
  - Configuring security profiles to provision portions of the system's security resources to user logical systems and the master logical system.

    Only the master administrator can create, change, and delete security profiles and bind them to logical systems.

Copyright © 2013, Juniper Networks, Inc.

NOTE: A user logical system administrator can configure interface, routing, and security resources allocated to his logical system.

- Creating logical interfaces to assign to user logical systems. (The user logical system administrator configures logical interfaces assigned to his logical system.)
- Viewing and managing user logical systems, as required, and deleting user logical systems. When a user logical system is deleted, its allocated reserved resources are released for use by other logical systems.
- Configuring IDP, AppTrack, application identification, and application firewall features. The master administrator can also use trace and debug at the root level, and he can perform commit rollbacks. The master administrator manages the master logical system and configures all the features that a user logical system administrator can configure for his or her own logical systems including routing instances, static routes, dynamic routing protocols, zones, security policies, screens, and firewall authentication.

Related Documentation

- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- *Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems*
- *Junos OS Logical Systems Library for Security Devices*

Understanding User Logical Systems and the User Logical System Administrator Role

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Logical systems allow a master administrator to partition an SRX Series device into discrete contexts called user logical systems. User logical systems are self-contained, private contexts, separate both from one another and from the master logical system. A user logical system has its own security, networking, logical interfaces, routing configurations, and one or more user logical system administrators.

When the master administrator creates a user logical system, he assigns one or more user logical system administrators to manage it. A user logical system administrator has a view of the device that is limited to his logical system. Although a user logical system is managed by a user logical system administrator, the master administrator has a global view of the device and access to all user logical systems. If necessary, the master administrator can manage any user logical system on the device.

The role and responsibilities of a user logical system administrator differ from those of the master administrator. As a user logical system administrator, you can access, configure, and view the configuration for your user logical system resources, but not those of other user logical systems or the master logical system.

Copyright © 2013, Juniper Networks, Inc.

As a user logical system administrator, you can:

- Configure zones, address books, security policies, user lists, custom services, and so forth, for your user logical system environment, based on the resources allocated to it.

  For example, if the master administrator allocates 40 zones to your user logical system, you can configure and administer those zones, but you cannot change the allocated number.
- Configure routing instances and assign allotted interfaces to them. Create static routes and add them to your routing instances. Configure routing protocols.
- Configure, enable, and monitor application firewall policy on your user logical system.
- Configure AppTrack.
- View all assigned logical interfaces and configure their attributes. The attributes that you configure for logical interfaces for your user logical system cannot be seen by other user logical system administrators.
- Run operational commands for your user logical system.

Related Documentation

- Understanding Logical Systems for SRX Series Services Gateways on page 3
- *Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems*
- *Understanding Logical System Security Profiles*
- *Example: Configuring Logical Systems Security Profiles*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

 Copyright © 2013, Juniper Networks, Inc.

CHAPTER 3

Security Features

Understanding Logical System Interfaces and Routing Instances

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Logical interfaces on the device are allocated among the user logical systems by the master administrator. The user logical system administrator configures the attributes of the interfaces, including IP addresses, and assigns them to routing instances and zones.

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. There can be multiple routing tables for a single routing instance—for example, unicast IPv4, unicast IPv6, and multicast IPv4 routing tables can exist in a single routing instance. Routing protocol parameters and options control the information in the routing tables.

Interfaces and routing instances can be configured in the master logical system and in user logical systems. Configuring an interface or routing instance in a logical system is the same as configuring an interface or routing instance on a device that is not configured for logical systems. Any routing instance created within a logical system is only applicable to that logical system.

Copyright © 2013, Juniper Networks, Inc.

The default routing instance, master, refers to the main inet.0 routing table in the logical system. The master routing instance is reserved and cannot be specified as a routing instance. Routes are installed in the master routing instance by default, unless a routing instance is specified. Configure global routing options and protocols for the master routing instance by including statements at the [**edit protocols**] and [**edit routing-options**] hierarchy levels in the logical system.

You can configure only virtual router routing instance type in a user logical system. Only one virtual private LAN service (VPLS) routing instance type can be configured on the device and it must be in the interconnect logical system.

The user logical system administrator can configure and view all attributes for an interface or routing instance in a user logical system. All attributes of an interface or routing instance in a user logical system are also visible to the master administrator.

Multicast is a "one source, many destinations" method of traffic distribution, which means the destinations needing to receive the information from a particular source receive the traffic stream. The master and user logical system administrators can configure a logical system to support multicast applications. The same multicast configurations to configure a device as a node in a multicast network can be used in a logical system.

Related Documentation

- Example: Configuring Interfaces and Routing Instances for a User Logical System on page 49
- User Logical System Configuration Overview on page 45
- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- *Junos OS Logical Systems Library for Security Devices*
- *Junos OS Interfaces Library for Security Devices*

Understanding Logical System Zones

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Security zones are logical entities to which one or more interfaces are bound. Security zones can be configured on the master logical system by the master administrator or on user logical systems by the user logical system administrator. On a logical system, the administrator can configure multiple security zones, dividing the network into network segments to which various security options can be applied.

The master administrator configures the maximum and reserved numbers of security zones for each user logical system. The user logical system administrator can then create security zones in the user logical system and assign interfaces to each security zone. From a user logical system, the user logical system administrator can use the **show system security-profile zones** command to view the number of security zones allocated to the user logical system and the **show interfaces** command to view the interfaces allocated to the user logical system.

Copyright © 2013, Juniper Networks, Inc.

NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of security zones applied to the master logical system. The number of zones configured in the master logical system count toward the maximum number of zones available on the device.

The master and user administrator can configure the following properties of a security zone in a logical system:

- Interfaces that are part of a security zone.
- Screen options—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.
- TCP-Reset—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.
- Host inbound traffic—This feature specifies the kinds of traffic that can reach the device from systems that are directly connected to its interfaces. 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.)

There are no preconfigured security zones in the master logical system or user logical system.

The management functional zone (MGT) can only be configured for the master logical system. There is only one management interface per device and that interface is allocated to the master logical system.

The **all** interface can only be assigned to a zone in the master logical system by the master administrator.

The user logical system administrator can configure and view all attributes for a security zone in a user logical system. All attributes of a security zone in a user logical system are also visible to the master administrator.

Related Documentation

- Example: Configuring Zones for a User Logical System on page 56
- User Logical System Configuration Overview on page 45
- *Understanding Logical System Security Profiles*
- Understanding Logical System Interfaces and Routing Instances on page 21
- *Security Zones and Interfaces Overview*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Understanding Logical System Screen Options

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Junos OS screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos OS then applies firewall policies, which can contain content filtering and IDP components, to the traffic that passes the screen filters.

All screen options available on the device are available in each logical system. Each user logical system administrator can configure screen options for their user logical system. The master administrator can configure screen options for the master logical system as well as all user logical systems.

The user logical system administrator can configure and view all screen options in a user logical system. All screen options in a user logical system are visible to the master administrator.

Related Documentation

- Example: Configuring Screen Options for a User Logical System on page 59
- User Logical System Configuration Overview on page 45
- *Attack Detection and Prevention Overview*
- *Junos OS Logical Systems Library for Security Devices*

Understanding Logical System Security Policies

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

- Security Policies in Logical Systems on page 24
- Application Timeouts on page 25
- Security Policy Allocation on page 25

Security Policies in Logical Systems

Security policies enforce rules for what traffic can pass through the firewall and actions that need to take place on the traffic as it passes through the firewall. From the perspective of security policies, traffic enters one security zone and exits another security zone.

By default, a logical system denies all traffic in all directions, including intra-zone and inter-zone directions. Through the creation of security policies, the logical system administrator can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from specified sources to specified destinations.

Security policies can be configured in the master logical system and in user logical systems. Configuring a security policy in a logical system is the same as configuring a security policy on a device that is not configured for logical systems. Any security policies, policy rules, address books, applications and application sets, and schedulers created within a logical system are only applicable to that logical system. Only predefined

Copyright © 2013, Juniper Networks, Inc.

applications and application sets, such as **junos-ftp**, can be shared between logical systems.

NOTE: In a logical system, you cannot specify global as either the from-zone or the to-zone in a security policy.

The user logical system administrator can configure and view all attributes for security policies in a user logical system. All attributes of a security policy in a user logical system are also visible to the master administrator.

Application Timeouts

The application timeout value set for an application determines the session timeout. Application timeout behavior is the same in a logical system as at the root level. However, user logical system administrators can use predefined applications in security policies but cannot modify the timeout value of predefined applications. This is because the predefined applications are shared by the master logical system and all user logical systems, so the user logical system administrator is not allowed to change its behavior. Application timeout values are stored in the application entry database and in the corresponding logical system TCP and UDP port-based timeout tables.

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 logical system TCP and UDP port-based timeout table is searched for a timeout value.
2. The root TCP and UDP port-based timeout table is searched for a timeout value.
3. The protocol-based default timeout table is searched for a timeout value.

Security Policy Allocation

The master administrator configures the maximum and reserved numbers of security policies for each user logical system. The user logical system administrator can then create security policies in the user logical system. From a user logical system, the user logical system administrator can use the **show system security-profile policy** command to view the number of security policies allocated to the user logical system.

NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of security policies applied to the master logical system. The number of policies configured in the master logical system count toward the maximum number of policies available on the device.

Related Documentation

- Example: Configuring Security Policies in a User Logical System on page 61
- *Understanding Logical System Security Profiles*

Copyright © 2013, Juniper Networks, Inc.

- User Logical System Configuration Overview on page 45
- *Security Policies Overview*
- *Understanding Policy Application Timeout Configuration and Lookup*
- *Junos OS Logical Systems Library for Security Devices*

Understanding Logical System Firewall Authentication

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. Junos OS enables administrators to restrict and permit firewall users to access protected resources (different zones) behind a firewall based on their source IP address and other credentials.

The master administrator is responsible for configuring access profiles in the master logical system. Access profiles store usernames and passwords of users or point to external authentication servers where such information is stored. Access profiles configured at the master logical system are available to all user logical systems.

The master administrator configures the maximum and reserved numbers of firewall authentications for each user logical system. The user logical system administrator can then create firewall authentications in the user logical system. From a user logical system, the user logical system administrator can use the **show system security-profile auth-entry** command to view the number of authentication resources allocated to the user logical system.

To configure the access profile, the master administrator uses the **profile** configuration statement at the [**edit access**] hierarchy level in the master logical system. The access profile can also include the order of authentication methods, LDAP or RADIUS server options, and session options.

The user logical system administrator can then associate the access profile with a security policy in the user logical system. The user logical system administrator also specifies the type of authentication:

- With pass-through authentication, a host or a user from one zone tries to access resources on another zone using an FTP, a Telnet, or an HTTP client. The device uses FTP, Telnet, or HTTP to collect username and password information, and subsequent traffic from the user or host is allowed or denied based on the result of this authentication.
- With Web authentication, users use HTTP to connect to an IP address on the device that is enabled for Web authentication and are prompted for the username and password. Subsequent traffic from the user or host to the protected resource is allowed or denied based on the result of this authentication.

 Copyright © 2013, Juniper Networks, Inc.

The user logical system administrator configures the following properties for firewall authentication in the user logical system:

- Security policy that specifies firewall authentication for matching traffic. Firewall authentication is specified with the **firewall-authentication** configuration statement at the [**edit security policies from-zone** *zone-name* **to-zone** *zone-name* **policy** *policy-name* **then permit**] hierarchy level.

  Users or user groups in an access profile who are allowed access by the policy can optionally be specified with the client-match configuration statement. (If no users or user groups are specified, any user who is successfully authenticated is allowed access.)

  For pass-through authentication, the access profile can optionally be specified and Web redirect (redirecting the client system to a webpage for authentication) can be enabled.

- Type of authentication (pass-through or Web authentication), default access profile, and success banner for the FTP, Telnet, or HTTP session. These properties are configured with the **firewall-authentication** configuration statement at the [**edit access**] hierarchy level.

- Host inbound traffic. Protocols, services, or both are allowed to access the logical system. The types of traffic are configured with the **host-inbound-traffic** configuration statement at the [**edit security zones security-zone** *zone-name*] or [**edit security zones security-zone** *zone-name* **interfaces** *interface-name*] hierarchy levels.

From a user logical system, the user logical system administrator can use the **show security firewall-authentication users** or **show security firewall-authentication history** commands to view the information about firewall users and history for the user logical system. From the master logical system, the master administrator can use the same commands to view information for the master logical system, a specific user logical system, or all logical systems.

Related Documentation

- *Example: Configuring Access Profiles*
- Example: Configuring Firewall Authentication for a User Logical System on page 64
- User Logical System Configuration Overview on page 45
- *Understanding Logical System Security Profiles*
- *Firewall User Authentication Overview*
- *Junos OS Logical Systems Library for Security Devices*

Understanding Route-Based VPN Tunnels in Logical Systems

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

A VPN connection can secure traffic that passes between a logical system and a remote site across a WAN. With route-based VPNs, you configure one or more security policies in a logical system to regulate the traffic flowing through a single IP Security (IPsec) tunnel. For each IPsec tunnel, there is one set of IKE and IPsec security associations (SAs) that must be configured at the root level by the master administrator.

Copyright © 2013, Juniper Networks, Inc.

NOTE: Only route-based VPNs are supported for logical systems. Policy-based VPNs are not supported.

In addition to configuring IKE and IPsec SAs for each VPN, the master administrator must also assign a secure tunnel (st0) interface to a user logical system. An st0 interface can only be assigned to a single user logical system. However, multiple user logical systems can each be assigned their own st0 interface.

NOTE: The st0 unit 0 interface should not be assigned to a logical system, as an SA cannot be set up for this interface.

The user logical system administrator can configure the IP address and other attributes of the st0 interface assigned to the user logical system. The user logical system administrator cannot delete an st0 interface assigned to their user logical system.

For route-based VPNs, a security policy refers to a destination address and not a specific VPN tunnel. For cleartext traffic in a user logical system to be sent to the VPN tunnel for encapsulation, the user logical system administrator must make the following configurations:

- Security policy that permits traffic to a specified destination.
- Static route to the destination with the st0 interface as the next hop.

When Junos OS looks up routes in the user logical system to find the interface to use to send traffic to the destination address, it finds a static route through the st0 interface. Traffic is routed to the VPN tunnel as long as the security policy action is permit.

The master logical system and a user logical system can share a route-based VPN tunnel. An st0 interface assigned to a user logical system can also be used by the master logical system. For the master logical system, the master administrator configures a security policy that permits traffic to the remote destination and a static route to the remote destination with the st0 interface as the next hop.

VPN monitoring is configured by the master administrator in the master logical system. For the VPN monitor source interface, the master administrator must specify the st0 interface; a physical interface for a user logical system cannot be specified.

Related Documentation

- *Understanding Route-Based IPsec VPNs*
- User Logical System Configuration Overview on page 45
- *Example: Configuring IKE and IPsec SAs for a VPN Tunnel*
- Example: Configuring a Route-Based VPN Tunnel in a User Logical System on page 68
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Understanding Logical System Network Address Translation

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either or both source and destination addresses in a packet may be translated. NAT can include the translation of port numbers as well as IP addresses.

Any combination of static, destination, or source NAT can be configured in the root or user logical systems. Configuring NAT in a logical system is the same as configuring NAT in a root system. The master administrator can configure and monitor NAT in the master logical system as well as any user logical system.

For each user logical system, the master administrator can configure the maximum and reserved numbers for the following NAT resources:

- Source NAT pools and destination NAT pools
- IP addresses in source NAT pools with and without port address translation
- Rules for source, destination, and static NAT
- Persistent NAT bindings
- IP addresses that support port overloading

From a user logical system, the user logical system administrator can use the operational command **show system security-profile** with a NAT option to view the number of NAT resources allocated to the user logical system.

NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of NAT resources applied to the master logical system. The number of resources configured in the master logical system count toward the maximum number of NAT resources available on the device.

From a user logical system, the user logical system administrator can use the **show security nat** command to view the information about NAT for the user logical system. From the master logical system, the master administrator can use the same command to view information for the master logical system, a specific user logical system, or all logical systems.

Related Documentation

- Example: Configuring Network Address Translation for a User Logical System on page 71
- User Logical System Configuration Overview on page 45
- *Understanding Logical System Security Profiles*
- *NAT Overview*

Copyright © 2013, Juniper Networks, Inc.

- *Junos OS Logical Systems Library for Security Devices*

IDP in Logical Systems Overview

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

A Junos OS Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through a logical system.

This topic includes the following sections:

IDP Policies

The master administrator configures IDP policies at the root level. Configuring an IDP policy for logical systems is similar to configuring an IDP policy on a device that is not configured for logical systems. This can include the configuration of custom attack objects.

NOTE: User logical system administrators cannot create or modify IDP policies for their user logical systems. Only the master administrator can create IDP policies and bind them to user logical systems through a logical systems security profile.

NOTE: The user logical system administrator can create security zones in the user logical system and assign interfaces to each security zone. Zones that are specific to user logical systems cannot be referenced in IDP policies configured by the master administrator. The master administrator can reference zones in the master logical system in an IDP policy configured for the master logical system.

The master administrator then specifies an IDP policy in the security profile that is bound to a logical system. To enable IDP in a logical system, the master administrator or user logical system administrator configures a security policy that defines the traffic to be inspected and specifies the **permit application-services idp** action.

Although the master administrator can configure multiple IDP policies, a logical system can have only one active IDP policy at a time. For user logical systems, the master administrator can either bind the same IDP policy to multiple user logical systems or bind a unique IDP policy to each user logical system. To specify the active IDP policy for the master logical system, the master administrator can *either* reference the IDP policy in the security profile that is bound to the master logical system or use the **active-policy** configuration statement at the [**edit security idp**] hierarchy level.

Copyright © 2013, Juniper Networks, Inc.

NOTE: A commit error is generated if an IDP policy is both configured in the security profile that is bound to the master logical system and specified with the active-policy configuration statement. Use only one method to specify the active IDP policy for the master logical system.

IDP Installation and Licensing for Logical Systems

A single IDP security package is installed for all logical systems on the device. The download and install options can only be executed at the root level. The same version of the IDP attack database is shared by all logical systems.

An idp-sig license must be installed at the root level. Once IDP is enabled at the root level, it can be used with any logical system on the device.

NOTE: IPv6 for IDP is not supported on logical systems.

Related Documentation

- Understanding IDP Features in Logical Systems on page 31
- *Example: Configuring an IDP Policy for a User Logical System*
- *Example: Configuring an IDP Policy for the Master Logical System*
- User Logical System Configuration Overview on page 45
- *Understanding Logical System Security Profiles*
- *IDP Policies Overview*
- *Junos OS Logical Systems Library for Security Devices*

Understanding IDP Features in Logical Systems

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This topic includes the following sections:

Copyright © 2013, Juniper Networks, Inc.

Rulebases

A single IDP policy can contain only one instance of any type of rulebase. The following IDP rulebases are supported for logical systems:

- The Intrusion prevention system (IPS) rulebase uses attack objects to detect known and unknown attacks. It detects attacks based on stateful signature and protocol anomalies.
- The application-level distributed denial-of-service (DDoS) rulebase defines parameters to protect servers such as DNS or HTTP. The application-level DDoS rulebase defines the source match condition for traffic that should be monitored and takes an action, such as drop the connection, drop the packet, or no action. It can also perform actions against future connections that use the same IP address.

NOTE: **Status monitoring for IPS and application-level DDoS is global to the device and not on a per logical system basis.**

Protocol Decoders

The Junos IDP module ships with a set of preconfigured protocol decoders. These protocol decoders have default settings for various protocol-specific contextual checks that they perform. The IDP protocol decoder configuration is global and applies to all logical systems. Only the master administrator at the root level can modify the settings at the [**edit security idp sensor-configuration**] hierarchy level.

SSL Inspection

IDP SSL inspection uses the Secure Sockets Layer (SSL) protocol suite to enable inspection of HTTP traffic encrypted in SSL.

SSL inspection configuration is global and applies to all logical systems on a device. SSL inspection can only be configured by the master administrator at the root level with the **ssl-inspection** configuration statement at the [**edit security idp sensor-configuration**] hierarchy level.

Inline Tap Mode

The inline tap mode feature provides passive, inline detection of Application Layer threats for traffic matching security policies that have the IDP application service enabled. When a device is in inline tap mode, packets pass through firewall inspection and are also copied to the independent IDP module. This allows the packets to get to the next service module without waiting for IDP processing results.

Inline tap mode is enabled or disabled for all logical systems at the root level by the master administrator. To enable inline tap mode, use the **inline-tap** configuration statement at the [**edit security forwarding-process application-services maximize-idp-sessions**] hierarchy level. Delete the inline tap mode configuration to switch the device back to regular mode.

Copyright © 2013, Juniper Networks, Inc.

NOTE: The device must be restarted when switching to inline tap mode or back to regular mode.

Multi-Detectors

When a new IDP security package is received, it contains attack definitions and a detector. After a new policy is loaded, it is also associated with a detector. If the policy being loaded has an associated detector that matches the detector already in use by the existing policy, the new detector is not loaded and both policies use a single associated detector. But if the new detector does not match the current detector, the new detector is loaded along with the new policy. In this case, each loaded policy will then use its own associated detector for attack detection.

The version of the detector is common to all logical systems.

Logging and Monitoring

Status monitoring options are available to the master administrator only. All status monitoring options under the **show security idp** and **clear security idp** CLI operational commands present global information, but not on a per logical system basis.

NOTE: SNMP monitoring for IDP is not supported on logical systems.

IDP generates event logs when an event matches an IDP policy rule in which logging is enabled.

The logical systems identification is added to the following types of IDP traffic processing logs:

- Attack logs. The following example shows an attack log for the ls-product-design logical system:

  Oct 12 17:33:32 8.0.0.254 RT_IDP: IDP_ATTACK_LOG_EVENT_LS: IDP: In ls-product-design at 1286930013, SIG Attack log <4.0.0.1/34327->5.0.0.1/21> for TCP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in policy Recommended. attack: repeat=0, action=IGNORE, threat-severity=MEDIUM, name=FTP:USER:ROOT, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:ls-product-design-untrust:ge-0/0/0.0->ls-product-design-trust:ge-0/0/1.0, packet-log-id: 65535 and misc-message -

- IP action logs. The following example shows an IP action log for the ls-product-design logical system:

  Oct 13 16:56:04 8.0.0.254 RT_IDP: IDP_ATTACK_LOG_EVENT_LS: IDP: In ls-product-design at 1287014163, TRAFFIC Attack log <25.0.0.1/34802->15.0.0.1/21> for TCP protocol and service SERVICE_NONE application NONE by rule 1 of rulebase IPS in policy Recommended. attack: repeat=0, action=TRAFFIC_IPACTION_NOTIFY, threat-severity=INFO, name=_, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0,

Copyright © 2013, Juniper Networks, Inc.

```
intf:ls-product-design-trust:ge-0/0/1.0->ls-product-design-untrust:plt0.3,
packet-log-id: 0 and misc-message -
```

- Application DDoS logs. The following example shows an application DDoS log for the ls-product-design logical system:

```
Oct 11 16:29:57 8.0.0.254 RT_IDP: IDP_APPDDOS_APP_ATTACK_EVENT_LS: DDOS
Attack in ls-product-design at 1286839797 on my-http,
<ls-product-design-untrust:ge-0/0/0.0:4.0.0.1:33738->ls-product-design-trust:ge-0/0/1.0:5.0.0.1:80>
for TCP protocol and service HTTP by rule 1 of rulebase DDOS in policy Recommended.
 attack: repeats 0 action DROP threat-severity INFO, connection-hit-rate 0,
context-name http-url-parsed, hit-rate 6, value-hit-rate 6 time-scope PEER time-count
 2  time-period 10 secs, context value:  ascii: /abc.html hex: 2f 61 62 63 2e 68 74 6d 6c
```

Related Documentation

- *Understanding IDP Policy Rulebases*
- *Understanding IDP Protocol Decoders*
- *IDP SSL Overview*
- *Understanding IDP Inline Tap Mode*
- *Understanding Multiple IDP Detector Support*
- *Understanding IDP Logging*
- *Junos OS Logical Systems Library for Security Devices*

Understanding Logical System Application Identification Services

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Predefined and custom application signatures identify an application by matching patterns in the first few packets of a session. Identifying applications provides the following benefits:

- Allows Intrusion Detection and Prevention (IDP) to apply appropriate attack objects to applications running on nonstandard ports.
- Improves performance by narrowing the scope of attack signatures for applications without decoders.
- Enables you to create detailed reports using AppTrack on applications passing through the device.

With logical systems, predefined and custom application signatures are global resources that are shared by all logical systems. The master administrator is responsible for downloading and installing predefined Juniper Networks application signatures and creating custom application and nested application signatures to identify applications that are not part of the predefined database.

Application identification is enabled by default.

The application system cache (ASC) saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. Each user logical system has its own ASC. A user logical system administrator can display

 Copyright © 2013, Juniper Networks, Inc.

the ASC entries for their logical system with the **show services application-identification application-system-cache** command. A user logical system administrator can use the **clear services application-identification application-system-cache** command to clear the ASC entries for their logical system.

The master administrator can display or clear ASC entries for any logical system. The master administrator can also display or clear global counters with the **show services application-identification counter** and **clear services application-identification counter** commands.

Related Documentation

- *Understanding Junos OS Application Identification Database*
- *Example: Updating the Junos OS Application Identification Extracted Application Package Automatically*
- *Configuring Junos OS Application Identification Custom Application Definitions*
- *Understanding IDP Application Identification*
- *Understanding the Application System Cache*
- *Verifying Application System Cache Statistics*
- *Junos OS Logical Systems Library for Security Devices*

Understanding Logical System Application Firewall Services

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

An application firewall enables administrators of logical systems to create security policies for traffic based on application identification defined by application signatures. The application firewall provides additional security protection against dynamic-application traffic that might not be adequately controlled by standard network firewall policies. The application firewall controls information transmission by allowing or blocking traffic originating from particular applications.

To configure an application firewall, you define a rule set that contains rules specifying the action to be taken on identified dynamic applications. The rule set is configured independently and assigned to a security policy. Each rule set contains at least two rules, a matched rule (consisting of match criteria and action) and a default rule.

- A matched rule defines the action to be taken on matching traffic. When traffic matches an application and other criteria specified in the rule, the traffic is allowed or blocked based on the action specified in the rule.
- A default rule is applied when traffic does not match any other rule in the rule set.

The master administrator can download a predefined application signature database from the Juniper Networks Security Engineering website or can define application signatures using the Junos OS configuration CLI. For more information about application identification and application signatures, see *Application Identification Feature Guide for Security Devices*.

Copyright © 2013, Juniper Networks, Inc.

Configuring an application firewall on a logical system is the same process as configuring an application firewall on a device that is not configured with logical systems. However, the application firewall applies only to the logical system for which it is configured. The master administrator can configure, enable, and monitor application firewalls on the master logical system and all user logical systems on a device. User logical system administrators can configure, enable, and monitor application firewalls only on the user logical systems for which they have access.

Related Documentation

- *Example: Configuring Application Firewall Services for a Master Logical System*
- Example: Configuring Application Firewall Services for a User Logical System on page 77
- *Junos OS Logical Systems Library for Security Devices*

Understanding Logical System Application Tracking Services

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

AppTrack is an application tracking tool that provides statistics for analyzing bandwidth usage of your network. When enabled, AppTrack collects byte, packet, and duration statistics for application flows in the specified zone. By default, when each session closes, AppTrack generates a message that provides the byte and packet counts and duration of the session, and sends it to the host device. The Security Threat Response Manager (STRM) retrieves the data and provides flow-based application visibility.

AppTrack can be enabled and configured within any logical system. Configuring AppTrack in a logical system is the same as configuring AppTrack on a device that is not configured for logical systems. An AppTrack configuration only applies to the logical system in which it is configured. The name of the logical system is added to AppTrack logs. The master administrator can configure AppTrack for any logical system while a user logical system administrator can only configure AppTrack for the logical system that they are logged into.

NOTE: **The system log configuration is global on the device and must be configured by the master administrator. The user logical system administrator cannot configure system logging for a logical system.**

Counters keep track of the number of log messages sent and logs that have failed. AppTrack counters are global to the device. The master administrator as well as user logical system administrators can view AppTrack counters with the **show security application-tracking counters** command.

Related Documentation

- *Understanding AppTrack*
- *Example: Configuring AppTrack*
- Example: Configuring AppTrack for a User Logical System on page 81
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Understanding Logical Systems in the Context of Chassis Cluster

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

The behavior of a chassis cluster whose nodes consist of SRX Series devices running logical systems is the same as that of a cluster whose SRX Series nodes in the cluster are not running logical systems. No difference exists between events that cause a node to fail over. In particular, if a link associated with a single logical system fails, then the device fails over to another node in the cluster.

The master administrator configures the chassis cluster (including both primary and secondary nodes) before he or she creates and configures the logical systems. Each node in the cluster has the same configuration, as is the case for nodes in a cluster not running logical systems. All logical system configurations are synchronized and replicated between both nodes in the cluster.

When you use SRX Series devices running logical systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Related Documentation

- *Example: Configuring Logical Systems in an Active/Passive Chassis Cluster*
- *Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6)*
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 8
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- *Chassis Cluster Overview*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

 Copyright © 2013, Juniper Networks, Inc.

CHAPTER 4

IPv6 Security Features

IPv6 Addresses in Logical Systems Overview

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

IP version 6 (IPv6) increases the size of an IP address from the 32 bits that compose an IPv4 address to 128 bits. Each extra bit given to an address doubles the size of its address space. IPv6 has a much larger address space than the soon-to-be exhausted IPv4 address space.

IPv6 addresses can be configured in logical systems for the following features:

- Interfaces
- Firewall authentication
- Flows
- Routing (BGP only)
- Zones and security policies
- Screen options
- Network Address Translation (except for interface NAT)
- Administrative operations such as Telnet, SSH, HTTPS, and other utilities
- Chassis clusters

NOTE: An IPv6 session consumes twice the memory of an IPv4 session. Therefore the number of sessions available for IPv6 is half the reserved and maximum quotas configured for the flow session resource in a security profile. Use the vty command **show usp flow resource usage cp-session** to check flow session usage.

Related Documentation

- *Understanding IP Version 6 (IPv6)*

Copyright © 2013, Juniper Networks, Inc.

- *About IPv6 Address Types and How Junos OS for SRX Series Services Gateway and J Series Devices Use Them*
- *Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems*
- *Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6)*
- Understanding IPv6 Dual-Stack Lite in Logical Systems on page 40
- *Junos OS Logical Systems Library for Security Devices*

Understanding IPv6 Dual-Stack Lite in Logical Systems

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

IPv6 dual-stack lite (DS-Lite) allows migration to an IPv6 access network without changing end-user software. IPv4 users can continue to access IPv4 internet content using their current hardware, while IPv6 users are able to access IPv6 content. A DS-Lite softwire initiator at the customer edge encapsulates IPv4 packets into IPv6 packets while a softwire concentrator decapsulates the IPv4-in-IPv6 packets and also performs IPv4 NAT translations.

A specific softwire concentrator and the set of softwire initiators that connect with that softwire concentrator can belong to only one logical system. The master administrator configures the maximum and reserved numbers of softwire initiators that can be connected to a softwire concentrator in a logical system using the **dslite-softwire-initiator** configuration statement at the [**edit system security-profile resources**] hierarchy level. The default maximum value is the system maximum; the default reserved value is 0.

NOTE: The master administrator can configure a security profile for the master logical system that specifies the maximum and reserved numbers of softwire initiators that can connect to a softwire concentrator configured for the master logical system. The number of softwire initiators configured in the master logical system count toward the maximum number of softwire initiators available on the device.

The user logical system administrator can configure softwire concentrators for their user logical system and the master administrator can configure softwire concentrators for the master logical system at the [**edit security softwires**] hierarchy level. The master administrator can also configure softwire concentrators for a user logical system at the [**edit logical-systems *logical-system* security softwires**] hierarchy level.

NOTE: The softwire concentrator IPv6 address can match an IPv6 address configured on either a physical interface or a loopback interface.

Related Documentation

- Example: Configuring IPv6 Dual-Stack Lite for a User Logical System on page 101
- *Understanding Logical System Security Profiles*

Copyright © 2013, Juniper Networks, Inc.

- *Understanding IPv6 Dual-Stack Lite*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 2

Configuration

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 5

Configuration Tasks

User Logical System Configuration Overview

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

When the master administrator creates a user logical system, he assigns a user logical system administrator to manage it. A user logical system can have multiple user logical system administrators.

As a user logical system administrator, you can access and view resources in your user logical system but not those of other user logical systems or the master logical system. You can configure resources allocated to your user logical system, but you cannot modify the numbers of allocated resources.

The following procedure lists the tasks that the user logical system administrator performs to configure resources in the user logical system:

1. Log in to the user logical system with the login and password configured by the master administrator:

   a. Telnet or SSH to the management IP address configured on the device. Log into the user logical system with the administrator login and password provided by the master administrator.

      You enter a UNIX shell in the user logical system configured by the master administrator.

   b. The presence of the > prompt indicates the CLI has started. The prompt is preceded by a string that contains your username, the hostname of the router, and the name of the user logical system. When the CLI starts, you are at the top level in operational mode. You enter configuration mode by entering the **configure** operational mode command. The CLI prompt changes from user@host: *logical-system* > to user@host: *logical-system*#.

      To exit the CLI and return to the UNIX shell, enter the **quit** command.

2. Configure the logical interfaces assigned to the user logical system by the master administrator. Configure one or more routing instances and the routing protocols and

Copyright © 2013, Juniper Networks, Inc.

options within each instance. See "Example: Configuring Interfaces and Routing Instances for a User Logical System" on page 49.

3. Configure security resources for the user logical system:

   a. Create zones for the user logical system and bind the logical interfaces to the zones. Address books can be created that are attached to zones for use in policies. See "Example: Configuring Zones for a User Logical System" on page 56.

   b. Configure screen options at the zone level. See "Example: Configuring Screen Options for a User Logical System" on page 59.

   c. Configure security policies between zones in the user logical system. See "Example: Configuring Security Policies in a User Logical System" on page 61.

      Custom applications or application sets can be created for specific types of traffic. To create a custom application, use the **application** configuration statement at the [**edit applications**] hierarchy level. To create an application set, use the **application-set** configuration statement at the [**edit applications**] hierarchy level.

   d. Configure firewall authentication. The master administrator creates access profiles in the master logical system. See *Example: Configuring Access Profiles*.

      The user logical system administrator then configures a security policy that specifies firewall authentication for matching traffic and configures the type of authentication (pass-through or Web authentication), default access profile, and success banner. See "Example: Configuring Firewall Authentication for a User Logical System" on page 64.

   e. Configure a route-based VPN tunnel to secure traffic between a user logical system and a remote site. The master administrator assigns a secure tunnel interface to the user logical system and configures IKE and IPsec SAs for the VPN tunnel. See *Example: Configuring IKE and IPsec SAs for a VPN Tunnel*.

      The user logical system administrator then configures a route-based VPN tunnel. See "Example: Configuring a Route-Based VPN Tunnel in a User Logical System" on page 68.

   f. Configure Network Address Translation (NAT). See "Example: Configuring Network Address Translation for a User Logical System" on page 71.

   g. Enable IDP. The master administrator configures IDP policies at the root level and specifies an IDP policy in the security profile that is bound to a logical system. See *Example: Configuring an IDP Policy for a User Logical System*.

      The user logical system administrator then enables IDP in a security policy. See "Example: Enabling IDP in a User Logical System Security Policy" on page 74.

   h. Display or clear application system cache (ASC) entries. See "Understanding Logical System Application Identification Services" on page 34.

 Copyright © 2013, Juniper Networks, Inc.

i. Configure application firewall services on a user logical system. See "Understanding Logical System Application Firewall Services" on page 35 and "Example: Configuring Application Firewall Services for a User Logical System" on page 77.

j. Configure the AppTrack application tracking tool. See "Example: Configuring AppTrack for a User Logical System" on page 81.

Related Documentation

- Example: Configuring User Logical Systems on page 83
- Understanding User Logical Systems and the User Logical System Administrator Role on page 18
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 6

User Logical System Security Features

Example: Configuring Interfaces and Routing Instances for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure interfaces and routing instances for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Determine which logical interfaces and, optionally, which logical tunnel interfaces are allocated to your user logical system by the master administrator. The master

Copyright © 2013, Juniper Networks, Inc.

administrator configures the logical tunnel interfaces. See "Understanding the Master Logical System and the Master Administrator Role" on page 17.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

This example configures the interfaces and routing instances described in Table 3 on page 50.

Table 3: User Logical System Interface and Routing Instance Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/5.1	• IP address 12.1.1.1/24 • VLAN ID 700

Routing instance	pd-vr1	• Instance type: virtual router
		• Includes interfaces ge-0/0/5.1 and lt-0/0/0.3
		• Static routes:
		  • 13.1.1.0/24 next-hop 10.0.1.3
		  • 14.1.1.0/24 next-hop 10.0.1.4
		  • 12.12.1.0/24 next-hop 10.0.1.1

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 interfaces ge-0/0/5 unit 1 family inet address 12.1.1.1/24
set interfaces ge-0/0/5 unit 1 vlan-id 700
set routing-instances pd-vr1 instance-type virtual-router
set routing-instances pd-vr1 interface ge-0/0/5.1
set routing-instances pd-vr1 interface lt-0/0/0.3
set routing-instances pd-vr1 routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set routing-instances pd-vr1 routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
set routing-instances pd-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
```

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 an interface and a routing instance in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```


Copyright © 2013, Juniper Networks, Inc.

2. Configure the logical interface for a user logical system.

```
[edit interfaces]
lsdesignadmin1@host:ls-product-design# set ge-0/0/5 unit 1 family inet address
  12.1.1.1/24
lsdesignadmin1@host:ls-product-design# set ge-0/0/5 unit 1 vlan-id 700
```

3. Configure the routing instance and assign interfaces.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 instance-type virtual-router
lsdesignadmin1@host:ls-product-design# set pd-vr1 interface ge-0/0/5.1
lsdesignadmin1@host:ls-product-design# set pd-vr1 interface lt-0/0/0.3
```

4. Configure static routes.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
  13.1.1.0/24 next-hop 10.0.1.3
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
  14.1.1.0/24 next-hop 10.0.1.4
lsdesignadmin1@host:ls-product-design# set pd-vr1 routing-options static route
  12.12.1.0/24 next-hop 10.0.1.1
```

Results From configuration mode, confirm your configuration by entering the **show interfaces** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

NOTE: The master administrator configures the lt-0/0/0.3 interface. Thus, the lt-0/0/0.3 configuration appears in the show interfaces output even though you did not configure this item.

```
lsdesignadmin1@host:ls-product-design# show interfaces
ge-0/0/5 {
    unit 1 {
        vlan-id 700;
        family inet {
            address 12.1.1.1/24;
        }
    }
}
    lt-0/0/0 {
        unit 3 {
            encapsulation ethernet;
            peer-unit 2;
            family inet {
                address 10.0.1.2/24;
            }
        }
    }
lsdesignadmin1@host:ls-product-design# show routing-instances
pd-vr1 {
    instance-type virtual-router;
```

Copyright © 2013, Juniper Networks, Inc.

```
    interface ge-0/0/5.1;
    interface lt-0/0/0.3;
    routing-options {
      static {
        route 13.1.1.0/24 next-hop 10.0.1.3;
        route 14.1.1.0/24 next-hop 10.0.1.4;
        route 12.12.1.0/24 next-hop 10.0.1.1;
      }
    }
  }
```

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

Related Documentation

- User Logical System Configuration Overview on page 45
- Understanding Logical System Interfaces and Routing Instances on page 21
- *Junos OS Interfaces Library for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring OSPF Routing Protocol for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure OSPF for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Configure logical interface ge-0/0/5.1. Assign ge-0/0/5.1 and lt-0/0/0.3 to the pd-vr1 routing instance. See "Example: Configuring Interfaces and Routing Instances for a User Logical System" on page 49.

Overview

In this example, you configure OSPF for the ls-product-design user logical system, shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

Copyright © 2013, Juniper Networks, Inc.

This example enables OSPF routing on the ge-0/0/5.1 and lt-0/0/0.3 interfaces in the ls-product-design user logical system. You configure the following routing policies to export routes from the Junos OS routing table into OSPF in the pd-vr1 routing instance:

- ospf-redist-direct—Routes learned from directly connected interfaces.
- ospf-redist-static—Static routes.
- ospf-to-ospf—Routes learned from OSPF.

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 policy-options policy-statement ospf-redist-direct from protocol direct
set policy-options policy-statement ospf-redist-direct then accept
set policy-options policy-statement ospf-redist-static from protocol static
set policy-options policy-statement ospf-redist-static then accept
set policy-options policy-statement ospf-to-ospf from protocol ospf
set policy-options policy-statement ospf-to-ospf then accept
set routing-instances pd-vr1 protocols ospf export ospf-redist-direct
set routing-instances pd-vr1 protocols ospf export ospf-redist-static
set routing-instances pd-vr1 protocols ospf export ospf-to-ospf
set routing-instances pd-vr1 protocols ospf area 0.0.0.1 interface ge-0/0/5.1
set routing-instances pd-vr1 protocols ospf area 0.0.0.1 interface lt-0/0/0.3
```

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 OSPF for the user logical system:

1. Log in to the user logical system as the user logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Create routing policies that accept routes.

```
[edit policy-options]
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-direct
    from protocol direct
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-direct
    then accept
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-static
    from protocol static
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-redist-static
    then accept
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-to-ospf from
    protocol ospf
lsdesignadmin1@host:ls-product-design# set policy-statement ospf-to-ospf then
    accept
```

Copyright © 2013, Juniper Networks, Inc.

3. Apply the routing policies to routes exported from the Junos OS routing table into OSPF.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
  ospf-redist-direct
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
  ospf-redist-static
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf export
  ospf-to-ospf
```

4. Enable OSPF on the logical interfaces.

```
[edit routing-instances]
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf area 0.0.0.1
  interface ge-0/0/5.1
lsdesignadmin1@host:ls-product-design# set pd-vr1 protocols ospf area 0.0.0.1
  interface lt-0/0/0.3
```

Results From configuration mode, confirm your configuration by entering the **show policy-options** and **show routing-instances** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show policy-options
  policy-statement ospf-redist-direct {
    from protocol direct;
    then accept;
  }
  policy-statement ospf-redist-static {
    from protocol static;
    then accept;
  }
  policy-statement ospf-to-ospf {
    from protocol ospf;
    then accept;
  }
[edit]
lsdesignadmin1@host:ls-product-design# show routing-instances
  pd-vr1 {
    ...
    protocols {
      ospf {
        export [ ospf-redist-direct ospf-to-ospf ospf-redist-static ];
        area 0.0.0.1 {
          interface lt-0/0/0.3;
          interface ge-0/0/5.1;
        }
      }
    }
  }
```


Copyright © 2013, Juniper Networks, Inc.

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

Verification

Confirm that the configuration is working properly.

Verifying OSPF Interfaces

Purpose Verify OSPF-enabled interfaces.

Action From the CLI, enter the **show ospf interface instance pd-vr1** command.

```
lsdesignadmin1@host:ls-product-design> show ospf interface instance pd-vr1
Interface           State   Area            DR ID           BDR ID          Nbrs
lt-0/0/0.3          DR      0.0.0.0         10.0.1.2        0.0.0.0            0
ge-0/0/5.1          DR      0.0.0.1         10.0.1.2        0.0.0.0            0
```

Verifying OSPF Neighbors

Purpose Verify OSPF neighbors.

Action From the CLI, enter the **show ospf neighbor instance pd-vr1** command.

```
lsdesignadmin1@host:ls-product-design> show ospf neighbor instance pd-vr1
Address   Interface  State   ID     Pri Dead
10.0.1.1  plt0.1    Full    0.0.0.0    128   39
```

Verifying OSPF Routes

Purpose Verify OSPF routes.

Action From the CLI, enter the **show ospf route instance pd-vr1** command.

```
lsdesignadmin1@host:ls-product-design> show ospf route instance pd-vr1
Topology default Route Table:

Prefix             Path  Route      NH       Metric NextHop       Nexthop
                   Type  Type       Type            Interface     Address/LSP
10.0.1.0/24         Intra Network    IP             1 lt-0/0/0.3
12.12.1.0/24        Intra Network    IP             1 ge-0/0/5.1
```

Related Documentation

- Understanding Logical System Interfaces and Routing Instances on page 21
- *Example: Configuring OSPF Routing Protocol for the Master Logical System*
- *OSPF Configuration Overview*
- *Verifying an OSPF Configuration*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Example: Configuring Zones for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure zones for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Use the **show system security-profile zones** command to see the zone resources allocated to the logical system.
- Logical interfaces for the user logical system must be configured. See "Example: Configuring Interfaces and Routing Instances for a User Logical System" on page 49.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

This example creates the zones and address books described in Table 4 on page 56.

Table 4: User Logical System Zone and Address Book Configuration

Feature	Name	Configuration Parameters
Zones	ls-product-design-trust	• Bind to interface ge-0/0/5.1. • TCP reset enabled.
	ls-product-design-untrust	• Bind to interface lt-0/0/0.3.
Address books	product-design-internal	• Address product-designers: 12.1.1.0/24 • Attach to zone ls-product-design-trust
	product-design-external	• Address marketing: 13.1.1.0/24 • Address accounting: 14.1.1.0/24 • Address others: 12.12.1.0/24 • Address set otherlsys: marketing, accounting • Attach to zone ls-product-design-untrust

Copyright © 2013, Juniper Networks, Inc.

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 security address-book product-design-internal address product-designers 12.1.1.0/24
set security address-book product-design-internal attach zone ls-product-design-trust
set security address-book product-design-external address marketing 13.1.1.0/24
set security address-book product-design-external address accounting 14.1.1.0/24
set security address-book product-design-external address others 12.12.1.0/24
set security address-book product-design-external address-set otherlsys address
  marketing
set security address-book product-design-external address-set otherlsys address
  accounting
set security address-book product-design-external attach zone ls-product-design-untrust
set security zones security-zone ls-product-design-trust tcp-rst
set security zones security-zone ls-product-design-trust interfaces ge-0/0/5.1
set security zones security-zone ls-product-design-untrust interfaces lt-0/0/0.3
```

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 zones in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure a security zone and assign it to an interface.

   ```
   [edit security zones]
   lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-trust
     interfaces ge-0/0/5.1
   ```

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

   ```
   [edit security zones security-zone ls-product-design-trust]
   lsdesignadmin1@host:ls-product-design# set tcp-rst
   ```

4. Configure a security zone and assign it to an interface.

   ```
   [edit security zones]
   lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-untrust
     interfaces lt-0/0/0.3
   ```

5. Create global address book entries.

   ```
   [edit security]
   lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
     address product-designers 12.1.1.0/24
   lsdesignadmin1@host:ls-product-design# set address-book product-design-external
     address marketing 13.1.1.0/24
   ```

Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address accounting 14.1.1.0/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address others 12.12.1.0/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address-set otherlsys address marketing
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address-set otherlsys address accounting
```

6. Attach address books to zones.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
  attach zone ls-product-design-trust
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  attach zone ls-product-design-untrust
```

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

```
lsdesignadmin1@host:ls-product-design# show security
  address-book {
    product-design-internal {
      address product-designers 12.1.1.0/24;
      attach {
        zone ls-product-design-trust;
      }
    }
    product-design-external {
      address marketing 13.1.1.0/24;
      address accounting 14.1.1.0/24;
      address others 12.12.1.0/24;
      address-set otherlsys {
        address marketing;
        address accounting;
      }
      attach {
        zone ls-product-design-untrust;
      }
    }
  }
    zones {
      security-zone ls-product-design-trust {
        tcp-rst;
        interfaces {
          ge-0/0/5.1;
        }
      }
      security-zone ls-product-design-untrust {
        interfaces {
          lt-0/0/0.3;
        }
      }
    }
```


Copyright © 2013, Juniper Networks, Inc.

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

Related Documentation

- Understanding Logical System Zones on page 22
- User Logical System Configuration Overview on page 45
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring Screen Options for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure screen options for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Configure zones for the user logical system. See "Example: Configuring Zones for a User Logical System" on page 56.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

You can limit the number of concurrent sessions to the same destination IP address in a user logical system. Setting a destination-based session limit can ensure that Junos OS allows only an acceptable number of concurrent connection requests—no matter what the source—to reach any one host. When the number of concurrent connection requests to an IP address surpasses the limit, Junos OS blocks further connection attempts to that IP address. This example creates the screen options described in Table 5 on page 59.

Table 5: User Logical System Screen Options Configuration

Name	Configuration Parameters
limit-destination-sessions	• Limits concurrent connection requests to destination IPs to 80. • Applied to ls-product-design-untrust zone.

Copyright © 2013, Juniper Networks, Inc.

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 security screen ids-option limit-destination-sessions limit-session destination-ip-based
  80
set security zones security-zone ls-product-design-untrust screen
  limit-destination-sessions
```

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 destination-based session limits in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure a screen option for a destination-based session limit.

   ```
   [edit security]
   lsdesignadmin1@host:ls-product-design# set screen ids-option
     limit-destination-sessions limit-session destination-ip-based 80
   ```

3. Set the security zone for the screen option.

   ```
   [edit security]
   lsdesignadmin1@host:ls-product-design# set zones security-zone
     ls-product-design-untrust screen limit-destination-sessions
   ```

Results

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

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

```
lsdesignadmin1@host:ls-product-design# show security screen
ids-option limit-destination-sessions {
   limit-session {
      destination-ip-based 80;
   }
}
lsdesignadmin1@host:ls-product-design# show security zones
security-zone ls-product-design-trust {
   ...
}
   security-zone ls-product-design-untrust {
```


Copyright © 2013, Juniper Networks, Inc.

```
        screen limit-destination-sessions;
        ...
    }
```

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

Related Documentation

- User Logical System Configuration Overview on page 45
- Understanding Logical System Screen Options on page 24
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring Security Policies in a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure security policies for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system.
- Configure zones and address books. See "Example: Configuring Zones for a User Logical System" on page 56.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

This example configures the security policies described in Table 6 on page 62.

Copyright © 2013, Juniper Networks, Inc.

Table 6: User Logical System Security Policies Configuration

Name	Configuration Parameters
permit-all-to-otherlsys	Permit the following traffic: • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: product-designers • Destination address: otherlsys • Application: any
permit-all-from-otherlsys	Permit the following traffic: • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-designers • Application: any

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 security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy permit-all-to-otherlsys match source-address product-designers
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy permit-all-to-otherlsys match destination-address otherlsys
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy permit-all-to-otherlsys match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy permit-all-to-otherlsys then permit
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-all-from-otherlsys match destination-address product-designers
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-all-from-otherlsys match application any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-all-from-otherlsys 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 security policies in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
```


Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security policy that permits traffic from the ls-product-design-trust zone to the ls-product-design-untrust zone.

```
[edit security policies from-zone ls-product-design-trust to-zone
  ls-product-design-untrust]
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
  source-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
  destination-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
  application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys then
  permit
```

3. Configure a security policy that permits traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

```
[edit security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
  source-address otherlsys
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
  destination-address product-designers
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
  application any
lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys 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.

```
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy permit-all-to-otherlsys {
    match {
      source-address product-designers;
      destination-address otherlsys;
      application any;
    }
    then {
      permit;
    }
  }
}
  from-zone ls-product-design-untrust to-zone ls-product-design-trust {
    policy permit-all-from-otherlsys {
      match {
        source-address otherlsys;
        destination-address product-designers;
        application any;
      }
      then {
        permit;
```

```
        }
      }
    }
```

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

Verification

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

- Verifying Policy Configuration on page 64

Verifying Policy Configuration

Purpose Verify information about policies and rules.

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

Related Documentation

- Understanding Logical System Security Policies on page 24
- User Logical System Configuration Overview on page 45
- *Troubleshooting Security Policies*
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring Firewall Authentication for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure firewall authentication for a user logical system.

- Requirements on page 64
- Overview on page 65
- Configuration on page 65
- Verification on page 67

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Use the **show system security-profiles auth-entry** command to see the firewall authentication entries allocated to the logical system.
- Access profiles must be configured in the master logical system by the master administrator. See *Example: Configuring Access Profiles*.

Copyright © 2013, Juniper Networks, Inc.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

In this example, users in the ls-marketing-dept and ls-accounting-dept logical systems are required to authenticate when initiating certain connections to the product designers subnet. This example configures the firewall authentication described in Table 7 on page 65.

NOTE: This example uses the access profile configured in *Example: Configuring Access Profiles*and address book entries configured in "Example: Configuring Zones for a User Logical System" on page 56.

Table 7: User Logical System Firewall Authentication Configuration

Feature	Name	Configuration Parameters
Security policy	permit-authorized-users NOTE: Policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used. If you have previously configured a policy that permits traffic for the same from zone, to zone, source address, and destination address but with application **any**, the policy configured in this example would never be matched. (See "Example: Configuring Security Policies in a User Logical System" on page 61.) Therefore, this policy should be reordered so that it is checked first.	Permit firewall authentication for the following traffic: • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-engineers • Application: junos-h323 The ldap1 access profile is used for pass-through authentication.
Firewall authentication		• Pass-through authentication • HTTP login prompt "welcome" • Default access profile ldap1

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 security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-authorized-users match source-address otherlsys
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-authorized-users match destination-address product-designers
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-authorized-users match application junos-h323
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy permit-authorized-users then permit firewall-authentication pass-through
    access-profile ldap1
```

Copyright © 2013, Juniper Networks, Inc.

```
set access firewall-authentication pass-through default-profile ldap1
set access firewall-authentication pass-through http banner login “welcome”
```

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 firewall authentication in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure a security policy that permits firewall authentication.

   ```
   [edit security policies from-zone ls-product-design-untrust to-zone
     ls-product-design-trust]
   lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
     source-address otherlsys
   lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
     destination -address product-designers
   lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users match
     application junos-h323
   lsdesignadmin1@host:ls-product-design# set policy permit-authorized-users then
     permit firewall-authentication pass-through access-profile ldap1
   ```

3. Reorder the security policies.

   ```
   [edit]
   lsdesignadmin1@host:ls-product-design# insert security policies from-zone
     ls-product-design-untrust to-zone ls-product-design-trust policy
     permit-authorized-users before policy permit-all-from-otherlsys
   ```

4. Configure firewall authentication.

   ```
   [edit access firewall-authentication]
   lsdesignadmin1@host:ls-product-design# set pass-through http banner login
     "welcome"
   lsdesignadmin1@host:ls-product-design# set pass-through default-profile ldap1
   ```

Results

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

```
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
  policy permit-all-to-otherlsys {
    match {
      source-address product-designers;
      destination-address otherlsys;
      application any;
    }
    then {
      permit;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
}
  from-zone ls-product-design-untrust to-zone ls-product-design-trust {
    policy permit-authorized-users {
      match {
        source-address otherlsys;
        destination-address product-designers;
        application junos-h323;
      }
      then {
        permit {
          firewall-authentication {
            pass-through {
              access-profile ldap1;
            }
          }
        }
      }
    }
    policy permit-all-from-otherlsys {
      match {
        source-address otherlsys;
        destination-address product-designers;
        application any;
      }
      then {
        permit;
      }
    }
  }
lsdesignadmin1@host:ls-product-design# show access firewall-authentication
pass-through {
  default-profile ldap1;
  http {
    banner {
      login welcome;
    }
  }
}
```

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

Verification

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

- Verifying Firewall User Authentication and Monitoring Users and IP Addresses on page 67

Verifying Firewall User Authentication and Monitoring Users and IP Addresses

Purpose Display firewall authentication user history and verify the number of firewall users who successfully authenticated and firewall users who failed to log in.

Action From operational mode, enter these **show** commands.

Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design> show security firewall-authentication history
lsdesignadmin1@host:ls-product-design> show security firewall-authentication history
    identifier id
lsdesignadmin1@host:ls-product-design> show security firewall-authentication users
lsdesignadmin1@host:ls-product-design> show security firewall-authentication users
    identifier id
```

Related Documentation

- *Example: Configuring Access Profiles*
- Understanding Logical System Firewall Authentication on page 26
- User Logical System Configuration Overview on page 45
- *Example: Configuring Pass-Through Authentication*
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring a Route-Based VPN Tunnel in a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure a route-based VPN tunnel in a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Ensure that an st0 interface is assigned to the user logical system and IKE and IPsec SAs are configured at the root level by the master administrator. See *Example: Configuring IKE and IPsec SAs for a VPN Tunnel*.

Overview

In this example, you configure the ls-product-design user logical system as shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

You configure the route-based VPN parameters described in Table 8 on page 68.

Table 8: User Logical System Route-Based VPN Configuration

Feature	Name	Configuration Parameters
Tunnel interface	st0 unit 1	• IPv4 protocol family (inet) • IP address 10.11.11.150/24

Copyright © 2013, Juniper Networks, Inc.

Table 8: User Logical System Route-Based VPN Configuration *(continued)*

Feature	Name	Configuration Parameters
Static route		• Destination 192.168.168.0/24 • Next hop st0.1
Security policy	through-vpn	Permit the following traffic: • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: any • Destination address: 192.168.168.0/24 • Application: any

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 interfaces st0 unit 1 family inet address 10.11.11.150/24
set routing-options static route 192.168.168.0/24 next-hop st0.1
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy through-vpn match source-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy through-vpn match destination-address 192.168.168.0/24
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy through-vpn match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust
    policy through-vpn 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 route-based VPN tunnel in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   [edit]
   lsdesignadmin1@host:ls-product-design>configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure the VPN tunnel interface.

   ```
   [edit interfaces]
   lsdesignadmin1@host:ls-product-design# set st0 unit 1 family inet address
     10.11.11.150/24
   ```

3. Create a static route to the remote destination.

   ```
   [edit routing-options]
   ```

Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design# set static route 192.168.168.0/24 next-hop
  st0.1
```

4. Configure a security policy to permit traffic to the remote destination.

```
[edit security policies from-zone ls-product-design-trust to-zone
  ls-product-design-untrust]
lsdesignadmin1@host:ls-product-design# set policy through-vpn match
  source-address any
lsdesignadmin1@host:ls-product-design# set policy through-vpn match
  destination-address 192.168.168.0/24
lsdesignadmin1@host:ls-product-design# set policy through-vpn match application
  any
lsdesignadmin1@host:ls-product-design# set policy through-vpn then permit
```

Results From configuration mode, confirm your configuration by entering the **show interfaces st0**, **show routing-options**, 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]
lsdesignadmin1@host:ls-product-design# show interfaces st0
  unit 1 {
    family inet {
      address 10.11.11.150/24;
    }
  }
  lsdesignadmin1@host:ls-product-design# show routing-options
    static {
      route 192.168.168.0/24 next-hop st0.1;
    }
  [edit]
  lsdesignadmin1@host:ls-product-design# show security policies
    from-zone ls-product-design-trust to-zone ls-product-design-untrust {
      policy through-vpn {
        match {
          source-address any;
          destination-address 192.168.168.0/24;
          application any;
        }
        then {
          permit;
        }
      }
      ...
    }
```

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

Verification

Confirm that the configuration is working properly.

Copyright © 2013, Juniper Networks, Inc.

NOTE: Before starting the verification process, you need to send traffic from a host in the user logical system to a host in the 192.168.168.0/24 network. For example, initiate a ping from a host in the 12.1.1.1/24 subnet in the ls-product-design user logical system to the host 192.168.168.10.

- Verifying the IKE Phase 1 Status on page 71
- Verifying the IPsec Phase 2 Status on page 71

Verifying the IKE Phase 1 Status

Purpose Verify the IKE Phase 1 status.

Action From operational mode, enter the **show security ike security-associations** command. After obtaining an index number from the command, use the **show security ike security-associations index *index_number* detail** command.

For sample outputs and meanings, see the "Verification" section of *Example: Configuring a Route-Based VPN*.

Verifying the IPsec Phase 2 Status

Purpose Verify the IPsec Phase 2 status.

Action From operational mode, enter the **show security ipsec security-associations** command. After obtaining an index number from the command, use the **show security ipsec security-associations index *index_number* detail** command.

For sample outputs and meanings, see the "Verification" section of *Example: Configuring a Route-Based VPN*.

Related Documentation

- *Example: Configuring a Route-Based VPN*.
- Understanding Route-Based VPN Tunnels in Logical Systems on page 27
- User Logical System Configuration Overview on page 45
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring Network Address Translation for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure static NAT for a user logical system.

- Requirements on page 72
- Overview on page 72
- Configuration on page 72
- Verification on page 74

Copyright © 2013, Juniper Networks, Inc.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Use the **show system security-profile nat-static-rule** command to see the static NAT resources allocated to the logical system.
- Configure security policies. See "Example: Configuring Security Policies in a User Logical System" on page 61.

Overview

This example configures the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

Devices in the ls-product-design-untrust zone access a specific host in the ls-product-design-trust zone by way of the address 12.1.1.200/32. For packets that enter the ls-product-design logical system from the ls-product-design-untrust zone with the destination IP address 12.1.1.200/32, the destination IP address is translated to the 12.1.1.100/32. This example configures the static NAT described in Table 9 on page 72.

Table 9: User Logical System Static NAT Configuration

Feature	Name	Configuration Parameters
Static NAT rule set	rs1	• Rule r1 to match packets from the ls-product-design-untrust zone with destination address 12.1.1.200/32. • Destination IP address in matching packets is translated to 12.1.1.100/32.
Proxy ARP		Address 12.1.1.200 on interface lt-0/0/0.3.

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 security nat static rule-set rs1 from zone ls-product-design-untrust
set security nat static rule-set rs1 rule r1 match destination-address 12.1.1.200/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 12.1.1.100/32
set security nat proxy-arp interface lt-0/0/0.3 address 12.1.1.200/32
```


Copyright © 2013, Juniper Networks, Inc.

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 NAT in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a static NAT rule set.

```
[edit security nat static]
lsdesignadmin1@host:ls-product-design# set rule-set rs1 from zone
  ls-product-design-untrust
```

3. Configure a rule that matches packets and translates the destination address in the packets.

```
[edit security nat static]
lsdesignadmin1@host:ls-product-design# set rule-set rs1 rule r1 match
  destination-address 12.1.1.200/32
lsdesignadmin1@host:ls-product-design# set rule-set rs1 rule r1 then static-nat prefix
  12.1.1.100/32
```

4. Configure proxy ARP.

```
[edit security nat]
lsdesignadmin1@host:ls-product-design# set proxy-arp interface lt-0/0/0.3 address
  12.1.1.200/32
```

Results

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

```
lsdesignadmin1@host:ls-product-design# show security nat
static {
  rule-set rs1 {
    from zone ls-product-design-untrust;
    rule r1 {
      match {
        destination-address 12.1.1.200/32;
      }
      then {
        static-nat prefix 12.1.1.100/32;
      }
    }
  }
}
  proxy-arp {
    interface lt-0/0/0.3 {
      address {
        12.1.1.200/32;
      }
    }
```

Copyright © 2013, Juniper Networks, Inc.

```
}
```

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

Verification

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

- Verifying Static NAT Configuration on page 74
- Verifying NAT Application to Traffic on page 74

Verifying Static NAT Configuration

Purpose Verify that there is traffic matching the static NAT rule set.

Action From operational mode, enter the **show security nat static rule** command. View the Translation hits field to check for traffic that matches the rule.

Verifying NAT Application to Traffic

Purpose Verify that NAT is being applied to the specified traffic.

Action From operational mode, enter the **show security flow session** command.

Related Documentation

- User Logical System Configuration Overview on page 45
- Understanding Logical System Network Address Translation on page 29
- *Static NAT Configuration Overview*
- *Junos OS Logical Systems Library for Security Devices*

Example: Enabling IDP in a User Logical System Security Policy

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to enable IDP in a security policy in a user logical system.

- Requirements on page 74
- Overview on page 75
- Configuration on page 75
- Verification on page 76

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.

 Copyright © 2013, Juniper Networks, Inc.

- Use the **show system security-profiles idp-policy** command to see the security policy resources allocated to the logical system.
- Configure an IDP security policy for the user logical system as the master administrator. See *Example: Configuring an IDP Policy for a User Logical System*.

Overview

In this example, you configure the ls-product-design user logical system as shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

You enable IDP in a security policy that matches any traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone. Enabling IDP in a security policy directs matching traffic to be checked against the IDP rulebases.

NOTE: This example uses the IDP policy configured and assigned to the ls-product-design user logical system by the master administrator in *Example: Configuring an IDP Policy for a User Logical System*.

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 security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy enable-idp match source-address any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy enable-idp match destination-address any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy enable-idp match application any
set security policies from-zone ls-product-design-untrust to-zone ls-product-design-trust
    policy enable-idp then permit application-services idp
```

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 security policy to enable IDP in a user logical system:

1. Log in to the logical system as the user logical system administrator and enter configuration mode.

   ```
   [edit]
   lsdesignadmin1@host:ls-product-design>configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure a security policy that matches traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

Copyright © 2013, Juniper Networks, Inc.

```
[edit security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy enable-idp match source-address
  any
lsdesignadmin1@host:ls-product-design# set policy enable-idp match
  destination-address any
lsdesignadmin1@host:ls-product-design# set policy enable-idp match application
  any
```

3. Configure the security policy to enable IDP for matching traffic.

```
[edit security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set policy enable-idp then permit
  application-services idp
```

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.

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show security policies
  from-zone ls-product-design-untrust to-zone ls-product-design-trust {
    policy enable-idp {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            idp;
          }
        }
      }
    }
    ...
  }
```

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

Verification

Verifying Attack Matches

Purpose Verify that attacks are being matched in network traffic.

Action From operational mode, enter the **show security idp attack table** command.

```
admin@host> show security idp attack table
```


Copyright © 2013, Juniper Networks, Inc.

```
IDP attack statistics:
  Attack name                   #Hits
  FTP:USER:ROOT                    1
```

Related Documentation

- *Example: Configuring an IDP Policy for a User Logical System*
- IDP in Logical Systems Overview on page 30
- User Logical System Configuration Overview on page 45
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring Application Firewall Services for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example describes how to configure application firewall services on a user logical system by a user logical system administrator. User logical system administrators can manage and monitor their own system application firewall rule sets and rules and manage the dynamic applications allowed or blocked on their respective logical systems.

After configuring application firewall rule sets and rules, user logical system administrators add the application firewall rule set information to the security policy on their individual logical systems.

For information about configuring an application firewall within a security policy, see *Application Firewall Feature Guide for Security Devices*.

Requirements

Before you begin:

- Verify that the security zones are configured for the user logical system.
- Verify that the master administrator has allocated application firewall resources (appfw-rule-set and appfw-rule) in the security profile bound to the user logical system.

  For more information, see *Understanding Logical System Security Profiles*.
- Log in to the logical system as the user logical system administrator.

  For information about user logical system administrator role functions, see "Understanding User Logical Systems and the User Logical System Administrator Role" on page 18.

Copyright © 2013, Juniper Networks, Inc.

Overview

In this example you configure application firewall services on the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

This example creates the following application firewall configuration:

- Rule set, ls-product-design-rs1, with rules r1 and r2. When r1 is matched, Telnet traffic is allowed through the firewall. When r2 is matched, web traffic is allowed through the firewall.
- Rule set, ls-product-design-rs2, with rule r1. When r1 is matched, Facebook traffic is blocked by the firewall.

All rule sets require a default rule, which specifies whether to permit or deny traffic that is not specified in any rules of a rule set. The default-rule action (permit or deny) must be the opposite from the action that is specified for the other rule(s) in the rule set.

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 security application-firewall rule-sets ls-product-design-rs1 rule r1 match
    dynamic-application junos:TELNET
set security application-firewall rule-sets ls-product-design-rs1 rule r1 then permit
set security application-firewall rule-sets ls-product-design-rs1 rule r2 match
    dynamic-application-group junos:web
set security application-firewall rule-sets ls-product-design-rs1 rule r2 then permit
set security application-firewall rule-sets ls-product-design-rs1 default-rule deny
set security application-firewall rule-sets ls-product-design-rs2 rule r1 match
    dynamic-application junos:facebook
set security application-firewall rule-sets ls-product-design-rs2 rule r1 then deny
set security application-firewall rule-sets ls-product-design-rs2 default-rule permit
```

Step-by-Step Procedure

To configure application firewall for a user logical system:

1. Log in to the user logical system as the user logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure an application firewall rule set for this logical system.

   ```
   [edit]
   lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
       ls-product-design-rs1
   ```

3. Configure a rule for this rule set and specify which dynamic applications and dynamic application groups the rule should match.

   ```
   [edit]
   ```


Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
  ls-product-design-rs1 rule r1 match dynamic-application telnet then permit
```

4. Configure the default rule for this rule set and specify the action to take when the identified dynamic application is not specified in any rules of the rule set.

```
[edit]
lsdesignadmin1@host:ls-product-design# set security application-firewall rule-sets
  ls-product-design-rs1 default-rule deny
```

5. Repeat these steps to configure another rule set, ls-product-design-rs2, if desired.

Results From configuration mode, confirm your configuration by entering the **show security application-firewall rule-set all** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show security application-firewall rule-set all
...
  application-firewall {
    rule-sets ls-product-design-rs1 {
      rule r1 {
        match {
          dynamic-application [junos:TELNET];
        }
        then {
          permit;
        }
      }
      default-rule {
        deny;
      }
    }
    rule-sets ls-product-design-rs1 {
      rule r2 {
        match {
          dynamic-application-group [junos:web];
        }
        then {
          permit;
        }
      }
      rule-sets ls-product-design-rs2 {
        rule r1 {
          match {
            dynamic-application [junos:FACEBOOK];
          }
          then {
            deny;
          }
        }
        default-rule {
```

Copyright © 2013, Juniper Networks, Inc.

```
            permit;
        }
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying Application Firewall Configuration on page 80

Verifying Application Firewall Configuration

Purpose View the application firewall configuration on the user logical system.

Action From operational mode, enter the **show security application-firewall rule-set all** command.

```
lsdesignadmin1@host:ls-product-design> show security application-firewall rule-set all

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:TELNET
        Action:permit
        Number of sessions matched: 10
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 2

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r2
        Dynamic Applications: junos:web
        Action:permit
        Number of sessions matched: 20
Default rule:deny
        Number of sessions matched: 200
Number of sessions with appid pending: 4

Rule-set: ls-product-design-rs2
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:FACEBOOK
        Action:deny
        Number of sessions matched: 40
Default rule:permit
        Number of sessions matched: 400
Number of sessions with appid pending: 10
```

Related Documentation

- User Logical System Configuration Overview on page 45
- Understanding Logical System Application Firewall Services on page 35
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Example: Configuring AppTrack for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure the AppTrack tracking tool so you can analyze the bandwidth usage of your network.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- (Master administrator) Configure system logging in the master logical system. See *Network Monitoring and Troubleshooting Guide for Security Devices*.

Overview

This example shows how to enable application tracking for the security zone ls-product-design-trust in the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

The first message is generated at session start and update messages are sent every 5 minutes after that or until the session ends. A final message is sent at session end.

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 security zones security-zone ls-product-design-trust application-tracking
set security application-tracking first-update
```

Step-by-Step Procedure

To configure AppTrack for a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Enable AppTrack for the security zone.

   ```
   [edit security]
   ```

Copyright © 2013, Juniper Networks, Inc.

```
lsdesignadmin1@host:ls-product-design# set zones security-zone
  ls-product-design-trust application-tracking
```

3. Generate update messages at session start and at 5-minute intervals.

```
[edit security]
lsdesignadmin1@host:ls-product-design# set application-tracking first-update
```

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

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show security
...
  application-tracking {
    first-update;
  }
...
  zones {
    security-zone ls-product-design-trust {
      ...
      application-tracking;
    }
  }
```

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

Verification

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

- Verifying AppTrack Operation on page 82
- Verifying Security Flow Session Statistics on page 82
- Verifying Application System Cache Statistics on page 83
- Verifying the Status of Application Identification Counter Values on page 83

Verifying AppTrack Operation

Purpose View the AppTrack counters periodically to monitor tracking.

Action From operational mode, enter the **show application-tracking counters** command.

Verifying Security Flow Session Statistics

Purpose Compare byte and packet counts in logged messages with the session statistics from the **show security flow session** command output.

Copyright © 2013, Juniper Networks, Inc.

Action From operational mode, enter the **show security flow session** command.

Verifying Application System Cache Statistics

Purpose Compare cache statistics such as IP address, port, protocol, and service for an application from the **show services application-identification application-system-cache** command output.

Action From operational mode, enter the **show services application-identification application-system-cache** command.

Verifying the Status of Application Identification Counter Values

Purpose Compare session statistics for application identification counter values from the **show services application-identification counter** command output.

Action From operational mode, enter the **show services application-identification counter** command.

Related Documentation

- Understanding Logical System Application Tracking Services on page 36
- User Logical System Configuration Overview on page 45
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring User Logical Systems

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows the configuration of interfaces, routing instances, zones, and security policies for user logical systems.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Be sure you know which logical interfaces and optionally, which logical tunnel interface (and its IP address) are allocated to your user logical system by the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 17.

Copyright © 2013, Juniper Networks, Inc.

Overview

This example configures the ls-marketing-dept and ls-accounting-dept user logical systems shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*.

This example configures the parameters described in Table 10 on page 84 and Table 11 on page 85.

Table 10: ls-marketing-dept Logical System Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/6.1	• IP address 13.1.1.1/24 • VLAN ID 800

Routing instance	mk-vr1	• Instance type: virtual router
		• Includes interfaces ge-0/0/6.1 and lt-0/0/0.5
		• Static routes:
		  ◦ 12.1.1.0/24 next-hop 10.0.1.2
		  ◦ 14.1.1.0/24 next-hop 10.0.1.4
		  ◦ 12.12.1.0/24 next-hop 10.0.1.1

Zones	ls-marketing-trust	Bind to interface ge-0/0/6.1.
	ls-marketing-untrust	Bind to interface lt-0/0/0.5
Address books	marketing-internal	• Address marketers: 13.1.1.0/24 • Attach to zone ls-marketing-trust
	marketing-external	• Address design: 12.1.1.0/24 • Address accounting: 14.1.1.0/24 • Address others: 12.12.1.0/24 • Address set otherlsys: design, accounting • Attach to zone ls-marketing-untrust
Policies	permit-all-to-otherlsys	Permit the following traffic: • From zone: ls-marketing-trust • To zone: ls-marketing-untrust • Source address: marketers • Destination address: otherlsys • Application: any
	permit-all-from-otherlsys	Permit the following traffic: • From zone: ls-marketing-untrust • To zone: ls-marketing-trust • Source address: otherlsys • Destination address: marketers • Application: any

Copyright © 2013, Juniper Networks, Inc.

Table 11: ls-accounting-dept Logical System Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/7.1	• IP address 14.1.1.1/24 • VLAN ID 900

Routing instance	acct-vr1	• Instance type: virtual router
		• Includes interfaces ge-0/0/7.1 and lt-0/0/0.7
		• Static routes:
		  ◦ 12.1.1.0/24 next-hop 10.0.1.2
		  ◦ 13.1.1.0/24 next-hop 10.0.1.3
		  ◦ 12.12.1.0/24 next-hop 10.0.1.1

Zones	ls-accounting-trust	Bind to interface ge-0/0/7.1.
	ls-accounting-untrust	Bind to interface lt-0/0/0.7
Address books	accounting-internal	• Address accounting: 14.1.1.0/24 • Attach to zone ls-accounting-trust
	accounting-external	• Address design: 12.1.1.0/24 • Address marketing: 13.1.1.0/24 • Address others: 12.12.1.0/24 • Address set otherlsys: design, marketing • Attach to zone ls-accounting-untrust
Policies	permit-all-to-otherlsys	Permit the following traffic: • From zone: ls-accounting-trust • To zone: ls-accounting-untrust • Source address: accounting • Destination address: otherlsys • Application: any
	permit-all-from-otherlsys	Permit the following traffic: • From zone: ls-accounting-untrust • To zone: ls-accounting-trust • Source address: otherlsys • Destination address: accounting • Application: any

Configuration

- Configuring the ls-marketing-dept User Logical System on page 86
- Configuring the ls-accounting-dept User Logical System on page 89

Copyright © 2013, Juniper Networks, Inc.

Configuring the ls-marketing-dept User Logical System

CLI Quick Configuration

To quickly configure this section of the 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 interfaces ge-0/0/6 unit 1 family inet address 13.1.1.1/24
set interfaces ge-0/0/6 unit 1 vlan-id 800
set routing-instances mk-vr1 instance-type virtual-router
set routing-instances mk-vr1 interface ge-0/0/6.1
set routing-instances mk-vr1 interface lt-0/0/0.5
set routing-instances mk-vr1 routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances mk-vr1 routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
set routing-instances mk-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
set security zones security-zone ls-marketing-trust interfaces ge-0/0/6.1
set security zones security-zone ls-marketing-untrust interfaces lt-0/0/0.5
set security address-book marketing-external address design 12.1.1.0/24
set security address-book marketing-external address accounting 14.1.1.0/24
set security address-book marketing-external address others 12.12.1.0/24
set security address-book marketing-external address-set otherlsys address design
set security address-book marketing-external address-set otherlsys address accounting
set security address-book marketing-external attach zone ls-marketing-untrust
set security address-book marketing-internal address marketers 13.1.1.0/24
set security address-book marketing-internal attach zone ls-marketing-trust
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match source-address marketers
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match destination-address otherlsys
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys match application any
set security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust policy
  permit-all-to-otherlsys then permit
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match destination-address marketers
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys match application any
set security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust policy
  permit-all-from-otherlsys 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 user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsmarketingadmin1@host:ls-marketing-dept> configure
   lsmarketingadmin1@host:ls-marketing-dept#
   ```

2. Configure the logical interface for a user logical system.

Copyright © 2013, Juniper Networks, Inc.

```
[edit interfaces]
lsmarketingadmin1@host:ls-marketing-dept# set ge-0/0/6 unit 1 family inet address
  13.1.1.1/24
lsmarketingadmin1@host:ls-marketing-dept# set ge-0/0/6 unit 1 vlan-id 800
```

3. Configure the routing instance and assign interfaces.

```
[edit routing-instances]
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 instance-type virtual-router
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 interface ge-0/0/6.1
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 interface lt-0/0/0.5
```

4. Configure static routes.

```
[edit routing-instances]
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
  12.1.1.0/24 next-hop 10.0.1.2
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
  14.1.1.0/24 next-hop 10.0.1.4
lsmarketingadmin1@host:ls-marketing-dept# set mk-vr1 routing-options static route
  12.12.1.0/24 next-hop 10.0.1.1
```

5. Configure security zones and assign interfaces to each zone.

```
[edit security zones]
lsmarketingadmin1@host:ls-marketing-dept# set security-zone ls-marketing-trust
  interfaces ge-0/0/6.1
lsmarketingadmin1@host:ls-marketing-dept# set security-zone ls-marketing-untrust
  interfaces lt-0/0/0.5
```

6. Create address book entries.

```
[edit security]
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-internal
  address marketers 13.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  address design 12.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  address accounting 14.1.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  address others 12.12.1.0/24
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  address-set otherlsys address design
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  address-set otherlsys address accounting
```

7. Attach address books to zones.

```
[edit security]
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-internal
  attach zone ls-marketing-trust
lsmarketingadmin1@host:ls-marketing-dept# set address-book marketing-external
  attach zone ls-marketing-untrust
```

8. Configure a security policy that permits traffic from the ls-marketing-trust zone to the ls-marketing-untrust zone.

```
[edit security policies from-zone ls-marketing-trust to-zone ls-marketing-untrust]
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
  match source-address marketers
```

Copyright © 2013, Juniper Networks, Inc.

```
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
  match destination-address otherlsys
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys
  match application any
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-to-otherlsys then
  permit
```

9. Configure a security policy that permits traffic from the ls-marketing-untrust zone to the ls-marketing-trust zone.

```
[edit security policies from-zone ls-marketing-untrust to-zone ls-marketing-trust]
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
  match source-address otherlsys
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
  match destination-address marketers
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
  match application any
lsmarketingadmin1@host:ls-marketing-dept# set policy permit-all-from-otherlsys
  then permit
```

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

```
lsmarketingadmin1@host:ls-marketing-dept# show routing instances
  mk-vr1 {
    instance-type virtual-router;
    interface ge-0/0/6.1;
    interface lt-0/0/0.5;
    routing-options {
      static {
        route 12.1.1.0/24 next-hop 10.0.1.2;
        route 14.1.1.0/24 next-hop 10.0.1.4;
        route 12.12.1.0/24 next-hop 10.0.1.1;
      }
    }
  }
lsmarketingadmin1@host:ls-marketing-dept# show security
  address-book {
    marketing-external {
      address product-designers 12.1.1.0/24;
      address accounting 14.1.1.0/24;
      address others 12.12.1.0/24;
      address-set otherlsys {
        address product-designers;
        address accounting;
      }
      attach {
        zone ls-marketing-untrust;
      }
    }
    marketing-internal {
      address marketers 13.1.1.0/24;
      attach {
        zone ls-marketing-trust;
      }
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
    policies {
      from-zone ls-marketing-trust to-zone ls-marketing-untrust {
        policy permit-all-to-otherlsys {
          match {
            source-address marketers;
            destination-address otherlsys;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone ls-marketing-untrust to-zone ls-marketing-trust {
        policy permit-all-from-otherlsys {
          match {
            source-address otherlsys;
            destination-address marketers;
            application any;
          }
          then {
            permit;
          }
        }
      }
    }
    zones {
      security-zone ls-marketing-trust {
        interfaces {
          ge-0/0/6.1;
        }
      }
      security-zone ls-marketing-untrust {
        interfaces {
          lt-0/0/0.5;
        }
      }
    }
```

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

Configuring the ls-accounting-dept User Logical System

CLI Quick Configuration

To quickly configure this section of the 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 interfaces ge-0/0/7 unit 1 family inet address 14.1.1.1/24
set interfaces ge-0/0/7 unit 1 vlan-id 900
set routing-instances acct-vr1 instance-type virtual-router
set routing-instances acct-vr1 interface ge-0/0/7.1
set routing-instances acct-vr1 interface lt-0/0/0.7
```

Copyright © 2013, Juniper Networks, Inc.

```
set routing-instances acct-vr1 routing-options static route 12.12.1.0/24 next-hop 10.0.1.1
set routing-instances acct-vr1 routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances acct-vr1 routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set security address-book accounting-internal address accounting 14.1.1.0/24
set security address-book accounting-internal attach zone ls-accounting-trust
set security address-book accounting-external address design 12.1.1.0/24
set security address-book accounting-external address marketing 13.1.1.0/24
set security address-book accounting-external address others 12.12.1.0/24
set security address-book accounting-external address-set otherlsys address design
set security address-book accounting-external address-set otherlsys address marketing
set security address-book accounting-external attach zone ls-accounting-untrust
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
    permit-all-to-otherlsys match source-address accounting
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
    permit-all-to-otherlsys match destination-address otherlsys
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
    permit-all-to-otherlsys match application any
set security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust policy
    permit-all-to-otherlsys then permit
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
    permit-all-from-otherlsys match source-address otherlsys
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
    permit-all-from-otherlsys match destination-address accounting
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
    permit-all-from-otherlsys match application any
set security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust policy
    permit-all-from-otherlsys then permit
set security zones security-zone ls-accounting-trust interfaces ge-0/0/7.1
set security zones security-zone ls-accounting-untrust interfaces lt-0/0/0.7
```

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 user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsaccountingadmin1@host:ls-accounting-dept> configure
   lsaccountingadmin1@host:ls-accounting-dept#
   ```

2. Configure the logical interface for a user logical system.

   ```
   [edit interfaces]
   lsaccountingadmin1@host:ls-accounting-dept# set ge-0/0/7 unit 1 family inet
       address 14.1.1.1/24
   lsaccountingadmin1@host:ls-accounting-dept# set ge-0/0/7 unit 1 vlan-id 900
   ```

3. Configure the routing instance and assign interfaces.

   ```
   [edit routing-instances]
   lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 instance-type
       virtual-router
   lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 interface ge-0/0/7.1
   lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 interface lt-0/0/0.7
   ```


Copyright © 2013, Juniper Networks, Inc.

4. Configure static routes.

```
[edit routing-instances]
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 routing-options static
  route 12.1.1.0/24 next-hop 10.0.1.2
lsaccountingadmin1@host:ls-accounting-deptt# set acct-vr1 routing-options static
  route 13.1.1.0/24 next-hop 10.0.1.3
lsaccountingadmin1@host:ls-accounting-dept# set acct-vr1 routing-options static
  route 12.12.1.0/24 next-hop 10.0.1.1
```

5. Configure security zones and assign interfaces to each zone.

```
[edit security zones]
lsaccountingadmin1@host:ls-accounting-dept# set security-zone ls-accounting-trust
  interfaces ge-0/0/7.1
lsaccountingadmin1@host:ls-accounting-dept# set security-zone
  ls-accounting-untrust interfaces lt-0/0/0.7
```

6. Create address book entries.

```
[edit security]
lsaccountingadmin1@host:ls-accounting-dept# set address-book accounting-internal
  address accounting 14.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external address design 12.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external address marketing 13.1.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external address others 12.12.1.0/24
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external address-set otherlsys address design
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external address-set otherlsys address marketing
```

7. Attach address books to zones.

```
[edit security]
lsaccountingadmin1@host:ls-accounting-dept# set address-book accounting-internal
  attach zone ls-accounting-trust
lsaccountingadmin1@host:ls-accounting-dept# set address-book
  accounting-external attach zone ls-accounting-untrust
```

8. Configure a security policy that permits traffic from the ls-accounting-trust zone to the ls-accounting-untrust zone.

```
[edit security policies from-zone ls-accounting-trust to-zone ls-accounting-untrust]
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
  match source-address accounting
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
  match destination-address otherlsys
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
  match application any
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-to-otherlsys
  then permit
```

9. Configure a security policy that permits traffic from the ls-accounting-untrust zone to the ls-accounting-trust zone.

```
[edit security policies from-zone ls-accounting-untrust to-zone ls-accounting-trust]
```

Copyright © 2013, Juniper Networks, Inc.

```
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
  match source-address otherlsys
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
  match destination-address accounting
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
  match application any
lsaccountingadmin1@host:ls-accounting-dept# set policy permit-all-from-otherlsys
  then permit
```

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

```
lsaccountingadmin1@host:ls-accounting-dept# show routing-instances
acct-vr1 {
  instance-type virtual-router;
  interface ge-0/0/7.1;
  interface lt-0/0/0.7;
  routing-options {
    static {
      route 12.12.1.0/24 next-hop 10.0.1.1;
      route 12.1.1.0/24 next-hop 10.0.1.2;
      route 13.1.1.0/24 next-hop 10.0.1.3;
    }
  }
}
lsaccountingadmin1@host:ls-accounting-dept# show security
address-book {
  accounting-internal {
    address accounting 14.1.1.0/24;
    attach {
      zone ls-accounting-trust;
    }
  }
  accounting-external {
    address design 12.1.1.0/24;
    address marketing 13.1.1.0/24;
    address others 12.12.1.0/24;
    address-set otherlsys {
      address design;
      address marketing;
    }
    attach {
      zone ls-accounting-untrust;
    }
  }
}
  policies {
    from-zone ls-accounting-trust to-zone ls-accounting-untrust {
      policy permit-all-to-otherlsys {
        match {
          source-address accounting;
          destination-address otherlsys;
          application any;
        }
```


Copyright © 2013, Juniper Networks, Inc.

```
            then {
                permit;
            }
        }
    }
    from-zone ls-accounting-untrust to-zone ls-accounting-trust {
        policy permit-all-from-otherlsys {
            match {
                source-address otherlsys;
                destination-address accounting;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone ls-accounting-trust {
        interfaces {
            ge-0/0/7.1;
        }
    }
    security-zone ls-accounting-untrust {
        interfaces {
            lt-0/0/0.7;
        }
    }
}
```

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

Verification

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

- Verifying Policy Configuration on page 93

Verifying Policy Configuration

Purpose Verify information about policies and rules.

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

Related Documentation

- User Logical System Configuration Overview on page 45
- Understanding Logical System Interfaces and Routing Instances on page 21
- Understanding Logical System Zones on page 22
- Understanding Logical System Security Policies on page 24
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 7

IPv6 Security Features

Example: Configuring IPv6 Zones for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure IPv6 zones for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator.

  See "User Logical System Configuration Overview" on page 45.

- Ensure that forwarding options for inet6 is flow-based. Otherwise, you must configure it and reset the device.

  Use the **show security forwarding-options** command to check the configuration.

NOTE: **Only the user logical system administrator can configure the forwarding options.**

Overview

This example configures the ls-product-design user logical system described in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*

This example creates the IPv6 zones and address books described in Table 12 on page 96.

Copyright © 2013, Juniper Networks, Inc.

Table 12: User Logical System Zone and Address Book Configuration

Feature	Name	Configuration Parameters
Zones	ls-product-design-trust	• Bind to interface ge-0/0/5.1. • TCP reset enabled.
	ls-product-design-untrust	• Bind to interface lt-0/0/0.3.
Address books	product-design-internal	• Address product-designers: 3002::1/96 • Attach to zone ls-product-design-trust
	product-design-external	• Address marketing: 3003::1/24 • Address accounting: 3004::1/24 • Address others: 3002::2/24 • Address set otherlsys: marketing, accounting • Attach to zone ls-product-design-untrust

Configuration

CLI Quick Configuration

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

```
set logical-system lsys1 security address-book product-design-internal address
  product-designers 3002::1/96
set logical-system lsys1 security address-book product-design-internal attach zone
  ls-product-design-trust
set logical-system lsys1 security address-book product-design-external address marketing
  3003::1/24
set logical-system lsys1 security address-book product-design-external address accounting
  3004::1/24
set logical-system lsys1 security address-book product-design-external address others
  3002::2/24
set logical-system lsys1 security address-book product-design-external address-set
  otherlsys address marketing
set logical-system lsys1 security address-book product-design-external address-set
  otherlsys address accounting
set logical-system lsys1 security address-book product-design-external attach zone
  ls-product-design-untrust
set logical-system lsys1 security zones security-zone ls-product-design-trust tcp-rst
set logical-system lsys1 security zones security-zone ls-product-design-trust interfaces
  ge-0/0/5.1
set logical-system lsys1 security zones security-zone ls-product-design-untrust interfaces
  lt-0/0/0.3
```


Copyright © 2013, Juniper Networks, Inc.

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 IPv6 zones in a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

```
lsdesignadmin1@host:ls-product-design> configure
lsdesignadmin1@host:ls-product-design#
```

2. Configure a security zone and assign it to an interface.

```
[edit logical-system lsys1 security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-trust
  interfaces ge-0/0/5.1
```

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

```
[edit logical-system lsys1 security zones security-zone ls-product-design-trust]
lsdesignadmin1@host:ls-product-design# set tcp-rst
```

4. Configure a security zone and assign it to an interface.

```
[edit logical-system lsys1 security zones]
lsdesignadmin1@host:ls-product-design# set security-zone ls-product-design-untrust
  interfaces lt-0/0/0.3
```

5. Create global address book entries.

```
[edit logical-system lsys1 security]
lsdesignadmin1@host:ls-product-design# set address-book product-design-internal
  address product-designers 3002::1/96
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address marketing 3003::1/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address accounting 3004::1/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address others 3002::2/24
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address-set otherlsys address marketing
lsdesignadmin1@host:ls-product-design# set address-book product-design-external
  address-set otherlsys address accounting
```

6. Attach address books to zones.

```
[edit logical-system lsys1 security]
lsdesignadmin1@host:ls-product-design#set address-book product-design-internal
  attach zone ls-product-design-trust
lsdesignadmin1@host:ls-product-design#set address-book product-design-external
  attach zone ls-product-design-untrust
```

Results

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

```
lsdesignadmin1@host:ls-product-design# show security zones
address-book {
```

Copyright © 2013, Juniper Networks, Inc.

```
    product-design-internal {
        address product-designers 3002::1/96;
        attach {
            zone ls-product-design-trust;
        }
    }
    product-design-external {
        address marketing 3003::1/24;
        address accounting 3004::1/24;
        address others 3002::2/24;
        address-set otherlsys {
            address marketing;
            address accounting;
        }
        attach {
            zone ls-product-design-untrust;
        }
    }
}
zones {
    security-zone ls-product-design-trust {
        tcp-rst;
        interfaces {
            ge-0/0/5.1;
        }
    }
    security-zone ls-product-design-untrust {
        interfaces {
            lt-0/0/0.3;
        }
    }
}
```

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

Related Documentation

- Understanding Logical System Zones on page 22
- User Logical System Configuration Overview on page 45
- *Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems*
- Example: Configuring IPv6 Security Policies for a User Logical System on page 98
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring IPv6 Security Policies for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

This example shows how to configure IPv6 security policies for a user logical system.

- Requirements on page 99
- Overview on page 99
- Configuration on page 99
- Verification on page 101

Copyright © 2013, Juniper Networks, Inc.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator.

  See "User Logical System Configuration Overview" on page 45.

- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system.
- Configure zones and address books.

  See "Example: Configuring IPv6 Zones for a User Logical System" on page 95

Overview

This example shows how to configure the security policies described in Table 13 on page 99.

Table 13: User Logical System Security Policies Configuration

Policy Name	Configuration Parameters
permit-all-to-otherlsys	Permit the following traffic: • From zone: ls-product-design-trust • To zone: ls-product-design-untrust • Source address: product-designers • Destination address: otherlsys • Application: any
permit-all-from-otherlsys	Permit the following traffic: • From zone: ls-product-design-untrust • To zone: ls-product-design-trust • Source address: otherlsys • Destination address: product-designers • Application: any

Configuration

CLI Quick Configuration

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

```
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
    ls-product-design-untrust policy permit-all-to-otherlsys match source-address
    product-designers
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
    ls-product-design-untrust policy permit-all-to-otherlsys match destination-address
    otherlsys
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
    ls-product-design-untrust policy permit-all-to-otherlsys match application any
```

Copyright © 2013, Juniper Networks, Inc.

```
set logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
  ls-product-design-untrust policy permit-all-to-otherlsys then permit
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust policy permit-all-from-otherlsys match source-address otherlsys
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust policy permit-all-from-otherlsys match destination-address
  product-designers
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
  ls-product-design-trust policy permit-all-from-otherlsys match application any
set logical-systems lsys1 security policies from-zone ls-product-design-untrust to-zone
  ls-product-d esign-trust policy permit-all-from-otherlsys 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 IPv6 security policies for a user logical system:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Configure a security policy that permits traffic from the ls-product-design-trust zone to the ls-product-design-untrust zone.

   ```
   [edit logical-systems lsys1 security policies from-zone ls-product-design-trust to-zone
     ls-product-design-untrust]
   lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
     source-address product-designers
   lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
     destination-address otherlsys
   lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys match
     application any
   lsdesignadmin1@host:ls-product-design# set policy permit-all-to-otherlsys then
     permit
   ```

3. Configure a security policy that permits traffic from the ls-product-design-untrust zone to the ls-product-design-trust zone.

   ```
   [edit logical-systems lsys1 security policies from-zone ls-product-design-untrust
     to-zone ls-product-design-trust]
   lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
     source-address otherlsys
   lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
     destination-address product-designers
   lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys match
     application any
   lsdesignadmin1@host:ls-product-design# set policy permit-all-from-otherlsys then
     permit
   ```


Copyright © 2013, Juniper Networks, Inc.

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.

```
lsdesignadmin1@host:ls-product-design# show security policies
from-zone ls-product-design-trust to-zone ls-product-design-untrust {
    policy permit-all-to-otherlsys {
        match {
            source-address product-designers;
            destination-address otherlsys;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone ls-product-design-untrust to-zone ls-product-design-trust {
    policy permit-all-from-otherlsys {
        match {
            source-address otherlsys;
            destination-address product-designers;
            application any;
        }
        then {
            permit;
        }
    }
}
```

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

Verification

Verifying Policy Configuration

Purpose Verify information about policies and rules.

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

Related Documentation

- Understanding Logical System Security Policies on page 24
- User Logical System Configuration Overview on page 45
- *Troubleshooting Security Policies*
- Example: Configuring IPv6 Zones for a User Logical System on page 95
- *Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems*
- *Junos OS Logical Systems Library for Security Devices*

Example: Configuring IPv6 Dual-Stack Lite for a User Logical System

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Copyright © 2013, Juniper Networks, Inc.

This example shows how to configure a softwire concentrator for a user logical system.

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical System Configuration Overview" on page 45.
- Use the **show system security-profile dslite-softwire-initiator** command to see the number softwire initiators that can be connected to a softwire concentrator in the logical system.

Overview

This example shows how to configure a softwire concentrator to decapsulate IPv4-in-IPv6 packets in the ls-product-design user logical system shown in *Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System*. The IPv6 address of the softwire concentrator is 3000::1 and the name of the softwire configuration is sc_1.

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 security softwires softwire-name sc_1 softwire-concentrator 3000::1 softwire-type
    IPv4-in-IPv6
```

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 an IPv6 DS-Lite softwire concentrator:

1. Log in to the user logical system as the logical system administrator and enter configuration mode.

   ```
   lsdesignadmin1@host:ls-product-design> configure
   lsdesignadmin1@host:ls-product-design#
   ```

2. Specify the address of the softwire concentrator and the softwire type.

   ```
   [edit security]
   lsdesignadmin1@host:ls-product-design# set softwires softwire-name sc_1
     softwire-concentrator 3000::1 softwire-type IPv4-in-IPv6
   ```


Copyright © 2013, Juniper Networks, Inc.

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

```
[edit]
lsdesignadmin1@host:ls-product-design# show security softwires
softwire-name sc_1 {
   softwire-concentrator 3000::1;
   softwire-type IPv4-in-IPv6;
}
```

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

Verification

Verifying the DS-Lite Configuration

Purpose Verify that the softwire initiators can connect to the softwire concentrator configured in the user logical system.

Action From operational mode, enter the **show security softwires** command.

If a softwire initiator is not connected, the operational output looks like this:

```
lsdesignadmin1@host:ls-product-design> show security softwires
Softwire Name            SC Address         Status   Number of SI connected
  sc_1                      3000::1         Active         0
```

If a softwire initiator is connected, the operational output looks like this:

```
lsdesignadmin1@host:ls-product-design> show security softwires
Softwire Name            SC Address         Status   Number of SI connected
  sc_1                      3000::1         Connected      1
```

Related Documentation

- Understanding IPv6 Dual-Stack Lite in Logical Systems on page 40
- User Logical System Configuration Overview on page 45
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 8

Configuration Statements for Security Features

Security Configuration Statement Hierarchy

Supported Platforms J Series, LN Series, SRX Series

Use the statements in the **security** configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones. Statements that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the **[edit security]** hierarchy.

- [edit security address-book] Hierarchy Level on page 106
- *[edit security alarms] Hierarchy Level*
- *[edit security alg] Hierarchy Level*

Copyright © 2013, Juniper Networks, Inc.

- *[edit security analysis] Hierarchy Level*
- [edit security application-firewall] Hierarchy Level on page 109
- [edit security application-tracking] Hierarchy Level on page 111
- *[edit security certificates] Hierarchy Level*
- *[edit security datapath-debug] Hierarchy Level*
- *[edit security dynamic-vpn] Hierarchy Level*
- [edit security firewall-authentication] Hierarchy Level on page 112
- [edit security flow] Hierarchy Level on page 113
- *[edit security forwarding-options] Hierarchy Level*
- *[edit security forwarding-process] Hierarchy Level*
- *[edit security gprs] Hierarchy Level*
- *[edit security group-vpn] Hierarchy Level*
- *[edit security idp] Hierarchy Level*
- *[edit security ike] Hierarchy Level*
- *[edit security ipsec] Hierarchy Level*
- *[edit security log] Hierarchy Level*
- [edit security nat] Hierarchy Level on page 117
- *[edit security pki] Hierarchy Level*
- [edit security policies] Hierarchy Level on page 124
- *[edit security resource-manager] Hierarchy Level*
- [edit security screen] Hierarchy Level on page 133
- [edit security softwires] Hierarchy Level on page 137
- *[edit security ssh-known-hosts] Hierarchy Level*
- *[edit security traceoptions] Hierarchy Level*
- *[edit security user-identification] Hierarchy Level*
- *[edit security utm] Hierarchy Level*
- [edit security zones] Hierarchy Level on page 139

Related Documentation

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *CLI User Guide*

[edit security address-book] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

Copyright © 2013, Juniper Networks, Inc.

```
security {
  address-book (book-name | global) {
    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;
    }
    attach {
      zone zone-name;
    }
    description text;
  }
}
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *MPLS Feature Guide for Security Devices*
- *Address Books and Address Sets Feature Guide for Security Devices*
- *Security Policy Applications Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

address-book

Supported Platforms J Series, LN Series, SRX Series

Syntax

```
address-book (book-name | global) {
  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;
  }
  attach {
    zone zone-name;
  }
  description text;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS. Statement moved under the security hierarchy in Release 11.2 of Junos OS. Support for address range added in Release 12.1 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

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.

Copyright © 2013, Juniper Networks, Inc.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Address Books and Address Sets Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

[edit security application-firewall] Hierarchy Level

Supported Platforms SRX Series

```
security {
  application-firewall {
    nested-application {
      dynamic-lookup {
        enable;
      }
    }
    profile profile-name {
      block-message type {
        custom-text content custom-html-text;
        custom-redirect-url content custom-redirect-url;
      }
    }
    rule-sets rule-set-name {
      default-rule {
        (deny [block-message] | permit | reject [block-message]);
      }
      profile profile-name;
      rule rule-name {
        match {
          dynamic-application [system-application];
          dynamic-application-group [system-application-group];
          ssl-encryption (any | yes | no);
        }
        then {
          (deny [block-message] | permit | reject [block-message]);
        }
      }
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag flag;
      no-remote-trace;
    }
  }
```

Copyright © 2013, Juniper Networks, Inc.

}

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Application Firewall Feature Guide for Security Devices*
- *Security Policy Applications Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

application-firewall

Supported Platforms SRX Series

Syntax

```
application-firewall {
  rule-sets rule-set-name {
    default-rule {
      (deny | permit);
    }
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-group [system-application-group];
      }
      then {
        (deny | permit);
      }
    }
  }
  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 Release 11.1 of Junos OS.

Description Configure application firewall rule sets with rules defining match criteria and the action to be performed.

Options The remaining statements are explained separately.

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

Related Documentation

- *Application Firewall Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

[edit security application-tracking] Hierarchy Level

Supported Platforms SRX Series

```
security {
  application-tracking {
    disable;
    (first-update | first-update-interval first-update-interval);
    session-update-interval session-update-interval;
  }
}
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Application Tracking Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

application-tracking

Supported Platforms SRX Series

Syntax

```
application-tracking {
  disable;
  (first-update | first-update-interval first-update-interval);
  session-update-interval session-update-interval;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 10.2. Support for **disable** added in Junos OS Release 11.4.

Description AppTrack, an application tracking tool, is a form of statistical profiling. Enabling this feature for a zone logs flow statistics (the byte count, packet count, and start and end times for a session) at session end. You can modify the logging time and log frequency with command options. Periodically, a network management tool, such as STRM, collects the logged statistics sent by each network device for bandwidth usage analysis of the network.

Options The remaining statements are explained separately.

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

Related Documentation

- *Application Tracking Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

[edit security firewall-authentication] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

```
security {
  firewall-authentication {
    traceoptions {
```


Copyright © 2013, Juniper Networks, Inc.

```
        flag flag;
      }
    }
  }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Junos OS Logical Systems Library for Security Devices*
- *Firewall User Authentication Feature Guide for Security Devices*

firewall-authentication (Security)

Supported Platforms J Series, LN Series, SRX Series

Syntax

```
firewall-authentication {
  traceoptions {
    flag flag;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.

Description Define data-plane firewall authentication tracing options.

Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.
  - **all**—Enable all tracing operations.
  - **authentication**—Trace data-plane firewall authentication events.
  - **proxy**—Trace data-plane firewall authentication proxy events.
- **detail**—Display moderate amount of data.
- **extensive**—Display extensive amount of data.
- **terse**—Display minimum amount of data.

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

Related Documentation

- *Firewall User Authentication Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

[edit security flow] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

```
security {
```

```
flow {
  aging {
    early-ageout seconds;
    high-watermark percent;
    low-watermark percent;
  }
  allow-dns-reply;
  bridge {
    block-non-ip-all;
    bpdu-vlan-flooding;
    bypass-non-ip-unicast;
    no-packet-flooding {
      no-trace-route;
    }
  }
  force-ip-reassembly;
  ipsec-performance-acceleration;
  load distribution {
    session-affinity ipsec;
  }
  pending-sess-queue-length (high | moderate | normal);
  route-change-timeout seconds;
  syn-flood-protection-mode (syn-cookie | syn-proxy);
  tcp-mss {
    all-tcp mss value;
    gre-in {
      mss value;
    }
    gre-out {
      mss value;
    }
    ipsec-vpn {
      mss value;
    }
  }
  tcp-session {
    fin-invalidate-session;
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    strict-syn-check;
    tcp-initial-timeout seconds;
    time-wait-state {
      (session-ageout | session-timeout seconds);
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
            flag flag;
            no-remote-trace;
            packet-filter filter-name {
               destination-port port-identifier;
               destination-prefix address;
               interface interface-name;
               protocol protocol-identifier;
               source-port port-identifier;
               source-prefix address;
            }
            rate-limit messages-per-second;
         }
      }
   }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Flow-Based Processing Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Network Monitoring and Troubleshooting Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

flow (Security Flow)

Supported Platforms J Series, LN Series, SRX Series

Syntax

```
flow {
  aging {
    early-ageout seconds;
    high-watermark percent;
    low-watermark percent;
  }
  allow-dns-reply;
  bridge {
    block-non-ip-all;
    bpdu-vlan-flooding;
    bypass-non-ip-unicast;
    no-packet-flooding {
      no-trace-route;
    }
  }
  force-ip-reassembly;
  ipsec-performance-acceleration;
  load distribution {
    session-affinity ipsec;
  }
  pending-sess-queue-length (high | moderate | normal);
  route-change-timeout seconds;
  syn-flood-protection-mode (syn-cookie | syn-proxy);
  tcp-mss {
    all-tcp mss value;
    gre-in {
      mss value;
    }
    gre-out {
      mss value;
    }
    ipsec-vpn {
      mss value;
    }
  }
  tcp-session {
    fin-invalidate-session;
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    strict-syn-check;
    tcp-initial-timeout seconds;
    time-wait-state {
      (session-ageout | session-timeout seconds);
    }
  }
  traceoptions {
    file {
      filename;
```


Copyright © 2013, Juniper Networks, Inc.

```
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
      packet-filter filter-name {
        destination-port port-identifier;
        destination-prefix address;
        interface interface-name;
        protocol protocol-identifier;
        source-port port-identifier;
        source-prefix address;
      }
      rate-limit messages-per-second;
    }
  }
```

Hierarchy Level [edit security]

Release Information Statement modified in Release 9.5 of Junos OS.

Description Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

- Enable or disable DNS replies when there is no matching DNS request.
- Set the initial session-timeout values.

Options The remaining statements are explained separately.

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

Related Documentation

- *Ethernet Port Switching Feature Guide for Security Devices*
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
- *Processing Overview Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

[edit security nat] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

```
security {
  nat {
    destination {
      pool pool-name {
        address <ip-address> {
          (port port-number | to ip-address);
        }
```

Copyright © 2013, Juniper Networks, Inc.

```
    description text;
    routing-instance (routing-instance-name | default);
  }
  rule-set rule-set-name {
    description text;
    from {
      interface [interface-name];
      routing-instance [routing-instance-name];
      zone [zone-name];
    }
    rule rule-name {
      description text;
      match {
        (destination-address ip-address| destination-address-name address-name);
        destination-port port-number;
        protocol [protocol-name-or-number];
        source-address [ip-address];
        source-address-name [address-name];
      }
      then {
        destination-nat (off | pool pool-name | rule-session-count-alarm
          (clear-threshold value | raise-threshold value));
      }
    }
  }
}
proxy-arp interface interface-name address ip-address;
  to ip-address;
}
proxy-ndp interface interface-name address ip-address;
  to ip-address;
}
source {
  address-persistent;
  interface (port-overloading off | port-overloading-factor number);
  pool pool-name {
    address ip-address {
      to ip-address;
    }
    address-pooling (paired | no-paired);
    address-shared;
    description text;
    host-address-base ip-address;
    overflow-pool (pool-name | interface);
    pool-utilization-alarm (clear-threshold value | raise-threshold value);
    port (no-translation | port-overloading-factor number | range (port-low | <to
      port-high>));
    routing-instance routing-instance-name;
  }
  pool-default-port-range lower-port-range to upper-port-range;
  pool-utilization-alarm (clear-threshold value | raise-threshold value);
  port-randomization disable;
  rule-set rule-set-name {
    description text;
    from {
      interface [interface-name];
```


Copyright © 2013, Juniper Networks, Inc.

```
            routing-instance [routing-instance-name];
            zone [zone-name];
        }
        rule rule-name {
            description text;
            match {
                (destination-address <ip-address> | destination-address-name
                    <address-name>);
                destination-port port-number;
                protocol [protocol-name-or-number];
                source-address [ip-address];
                source-address-name [address-name];
                source-port (port-or-low <to high>);
            }
            then source-nat;
                interface {
                    persistent-nat {
                        address-mapping;
                        inactivity-timeout seconds;
                        max-session-number value;
                        permit (any-remote-host | target-host | target-host-port);
                    }
                off;
                pool <pool-name>
                    persistent-nat
                        address-mapping;
                        inactivity-timeout seconds;
                        max-session-number number;
                        permit (any-remote-host | target-host | target-host-port);
                    }
                rule-session-count-alarm (clear-threshold value | raise-threshold value);
            }
        }
        to {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
        }
    }
}
static rule-set rule-set-name;
    description text;
    from {
        interface [interface-name];
        routing-instance [routing-instance-name];
        zone [zone-name];
    }
    rule rule-name {
        description text;
        match {
            (destination-address <ip-address> | destination-address-name
                <address-name>);
            destination-port (port-or-low | <to high>);
            source-address [ip-address];
            source-address-name [address-name];
            source-port (port-or-low <to high>);
```

```
                }
                then static-nat;
                  inet {
                    routing-instance (routing-instance-name | default);
                  }
                  prefix {
                    address-prefix;
                    mapped-port lower-port-range to upper-port-range;
                    routing-instance (routing-instance-name| default);
                  }
                  prefix-name {
                    address-prefix-name;
                    mapped-port lower-port-range to upper-port-range;
                    routing-instance (routing-instance-name | default);
                  }
                  rule-session-count-alarm (clear-threshold value | raise-threshold value);
                  }
                }
              }
            }
          }
          traceoptions {
            file {
              filename;
              files number;
              match regular-expression;
              (world-readable | no-world-readable);
              size maximum-file-size;
            }
            flag flag;
            no-remote-trace;
          }
        }
      }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Network Monitoring and Troubleshooting Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

nat

Supported Platforms J Series, LN Series, SRX Series

Syntax

```
nat {
  destination {
    pool pool-name {
      address ip-address {
        (port port-number | to ip-address);
      }
      description text;
      routing-instance routing-instance-name;
    }
    rule-set rule-set-name {
      description text;
      from {
        interface [interface-name];
        routing-instance [routing-instance-name];
        zone [zone-name];
      }
      rule rule-name {
        description text;
        match {
          (destination-address <ip-address> | destination-address-name <address-name>);
          destination-port port-number;
          protocol [protocol-name-or-number];
          source-address [ip-address];
          source-address-name [address-name];
        }
        then {
          destination-nat (off | pool pool-name);
        }
      }
    }
  }
  proxy-arp {
    interface interface-name {
      address ip-address {
        to ip-address;
      }
    }
  }
  proxy-ndp {
    interface interface-name {
      address ip-address {
        to ip-address;
      }
    }
  }
  source {
    address-persistent;
    interface {
      port-overloading {
        off;
      }
```

```
}
pool pool-name {
  address ip-address {
    to ip-address;
  }
  description text;
  host-address-base ip-address;
  overflow-pool (interface | pool-name);
  port {
    (no-translation | port-overloading-factor number | range port-low <to port-high>);
  }
  routing-instance routing-instance-name;
}
pool-default-port-range lower-port-range to upper-port-range;
pool-utilization-alarm {
  clear-threshold value;
  raise-threshold value;
}
port-randomization {
  disable;
}
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      (destination-address <ip-address> | destination-address-name <address-name>);
      destination-port port-number;
      protocol [protocol-name-or-number];
      source-address [ip-address];
      source-address-name [address-name];
    }
    then {
      source-nat {
        interface {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number value;
            permit (any-remote-host | target-host | target-host-port);
          }
        }
        off;
        pool {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number number;
            permit (any-remote-host | target-host | target-host-port);
          }
          pool-name;
```


Copyright © 2013, Juniper Networks, Inc.

```
                }
              }
            }
          }
          to {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
          }
        }
      }
      static {
        rule-set rule-set-name {
          description text;
          from {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
          }
          rule rule-name {
            description text;
            match {
              (destination-address ip-address | destination-address-name address-name);
            }
            then {
              static-nat {
                inet {
                  routing-instance (default | routing-instance-name);
                }
                prefix {
                  address-prefix;
                  routing-instance (default | routing-instance-name);
                }
                prefix-name {
                  address-prefix-name;
                  routing-instance (default | routing-instance-name);
                }
              }
            }
          }
        }
      }
      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 modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

Description Configure Network Address Translation (NAT) for SRX Series devices.

Options The remaining statements are explained separately.

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

Related Documentation
- *Junos OS Application Layer Gateways (ALGs) Library for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Network Monitoring and Troubleshooting Guide for Security Devices*

[edit security policies] Hierarchy Level

Supported Platforms J Series, SRX Series

```
security {
  policies {
    default-policy (deny-all | permit-all);
    from-zone zone-name to-zone zone-name {
      policy policy-name {
        description description;
        match {
          application {
            [application];
            any;
          }
          destination-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
            }
          destination-address-excluded;
          source-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
            }
          source-address-excluded;
          source-identity {
            [role-name];
            any;
            authenticated-user;
            unauthenticated-user;
            unknown-user;
          }
```


Copyright © 2013, Juniper Networks, Inc.

```
}
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;
        ssl-termination-profile profile-name;
      }
      web-authentication {
        client-match user-or-group-name;
      }
    }
    services-offload;
    tcp-options {
```

Copyright © 2013, Juniper Networks, Inc.

```
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
  }
  global {
    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 {
```


Copyright © 2013, Juniper Networks, Inc.

```
            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
              ssl-termination-profile profile-name
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
        }
        reject;
      }
    }
  }
  policy-rematch;
  policy-stats {
    system-wide (disable | enable);
  }
  traceoptions {
    file {
      filename;
      files number;
```

```
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
      }
    }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *MPLS Feature Guide for Security Devices*
- *Application Firewall Feature Guide for Security Devices*
- *Application Quality of Service Feature Guide for Security Devices*
- *Security Policies Feature Guide for Security Devices*
- *Junos OS VPN Library for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Unified Access Control Design and Implementation Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

policies

Supported Platforms J Series, SRX Series

Syntax

```
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name 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;
            }
```

Copyright © 2013, Juniper Networks, Inc.

```
            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;
              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;
          }
        }
        reject;
      }
    }
}
global {
  policy policy-name {
    description description;
    match {
      application {
        [application];
        any;
      }
      destination-address {
```


Copyright © 2013, Juniper Networks, Inc.

```
      [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;
            }
          }
          reject;
        }
      }
    }
    policy-rematch;
    policy-stats {
      system-wide (disable | enable) ;
    }
    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 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 added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.

Description Configure network security policies.

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

 Copyright © 2013, Juniper Networks, Inc.

Related Documentation

- *Application Quality of Service Feature Guide for Security Devices*
- *Security Policies Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Junos OS UTM Library for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*

[edit security screen] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

```
security {
    screen {
        ids-option screen-name {
            alarm-without-drop;
            description text;
            icmp {
                flood {
                    threshold number;
                }
                fragment;
                ipv6-malformed-header;
                ip-sweep {
                    threshold number;
                }
                large;
                ping-death;
            }
            ip {
                bad-option;
                block-frag;
                ipv6-extension-header {
                    AH-header;
                    ESP-header
                    HIP-header;
                    destination-header {
                        ILNP-nonce-option;
                        home-address-option;
                        line-identification-option;
                        tunnel-encapsulation-limit-option;
                        user-defined-option-type low | <to high>;
                    }
                    fragment-header;
                    hop-by-hop-header {
                        CALIPSO-option;
                        RPL-option;
                        SFM-DPD-option;
                        jumbo-payload-option;
                        quick-start-option;
                        router-alert-option;
                        user-defined-option-type low | <to high>;
                    }
```

Copyright © 2013, Juniper Networks, Inc.

```
        mobility-header;
        no-next-header;
        routing-header;
        shim6-header
        user-defined-option-type low | <to high>;
    }
    ipv6-extension-header-limit limit;
    ipv6-malformed-header;
    loose-source-route-option;
    record-route-option;
    security-option;
    source-route-option;
    spoofing;
    stream-option;
    strict-source-route-option;
    tear-drop;
    timestamp-option;
    unknown-protocol;
}
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
tcp {
    fin-no-ack;
    land;
    port-scan {
        threshold number;
    }
    syn-ack-ack-proxy {
        threshold number;
    }
    syn-fin;
    syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
            destination-address destination-address;
            source-address source-address;
        }
    }
    syn-frag;
    tcp-no-flag;
    tcp-sweep {
        threshold threshold number;
    }
    winnuke;
}
udp {
    flood {
        threshold number;
    }
    udp-sweep {
```


Copyright © 2013, Juniper Networks, Inc.

```
                threshold threshold number;
              }
            }
          }
        }
        traceoptions {
          file filename {
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
      }
    }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

screen (Security)

Supported Platforms J Series, SRX Series

Syntax

```
screen {
    ids-option screen-name {
        alarm-without-drop;
        description text;
        icmp {
            flood {
                threshold number;
            }
            fragment;
            ip-sweep {
                threshold number;
            }
            large;
            ping-death;
        }
        ip {
            bad-option;
            block-frag;
            loose-source-route-option;
            record-route-option;
            security-option;
            source-route-option;
            spoofing;
            stream-option;
            strict-source-route-option;
            tear-drop;
            timestamp-option;
            unknown-protocol;
        }
        limit-session {
            destination-ip-based number;
            source-ip-based number;
        }
        tcp {
            fin-no-ack;
            land;
            port-scan {
                threshold number;
            }
            syn-ack-ack-proxy {
                threshold number;
            }
            syn-fin;
            syn-flood {
                alarm-threshold number;
                attack-threshold number;
                destination-threshold number;
                source-threshold number;
                timeout seconds;
                white-list name {
                    destination-address destination-address;
```


Copyright © 2013, Juniper Networks, Inc.

```
            source-address source-address;
          }
        }
        syn-frag;
        tcp-no-flag;
        tcp-sweep {
          threshold threshold number;
        }
        winnuke;
      }
      udp {
        flood {
          threshold number;
        }
        udp-sweep {
          threshold threshold number;
        }
      }
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Release 8.5 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

Description Configure security screen options.

Options ***screen-name***—Name of the screen configured at the **security screen ids-options** level.

The remaining statements are explained separately.

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

Related Documentation

- *Junos OS Logical Systems Library for Security Devices*

[edit security softwires] Hierarchy Level

Supported Platforms LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Copyright © 2013, Juniper Networks, Inc.

```
security {
  softwires {
    softwire-name name {
      softwire-concentrator ipv6-address;
      softwire-type IPv4-in-IPv6;
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag (all | configuration | flow);
      no-remote-trace;
    }
  }
}
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Flow-Based Processing Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

softwires

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Syntax

```
softwires {
  softwire-name name {
    softwire-concentrator ipv6-address;
    softwire-type IPv4-in-IPv6;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | flow);
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Release 12.1 of Junos OS.

Description Configure softwires for IPv6 dual-stack lite (DS-Lite). DS-Lite allows migration to an IPv6 access network without changing end-user software. IPv4 users can continue to access IPv4 internet content using their current hardware, while IPv6 users are able to access IPv6 content.

Options

- **softwire-name *name***—Name of the softwire configuration.
  - **softwire-concentrator *ipv6-address***—IPv6 address of the concentrator.
  - **softwire-type**—Must be IPv4-in-IPv6.

The remaining statements are explained separately.

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

Related Documentation

- *Junos OS Logical Systems Library for Security Devices*

[edit security zones] Hierarchy Level

Supported Platforms J Series, LN Series, SRX Series

```
security {
  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;
    }
  }
  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;
```

 Copyright © 2013, Juniper Networks, Inc.

```
            }
            system-services service-name {
              except;
            }
          }
        }
        screen screen-name;
        tcp-rst;
      }
    }
  }
```

Related Documentation

- Security Configuration Statement Hierarchy on page 105
- *Application Tracking Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Unified Access Control Design and Implementation Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

zones

Supported Platforms J Series, LN Series, SRX Series

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;
      }
    }
    application-tracking;
    description text;
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
```


Copyright © 2013, Juniper Networks, Inc.

```
        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.

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

Related Documentation

- *Application Tracking Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 3

Administration

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 9

Operational Commands for Security Features

Copyright © 2013, Juniper Networks, Inc.

clear security application-firewall rule-set statistics logical-system

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Syntax The master, or root, administrator can issue the following statements:

clear security application-firewall rule-set statistics [logical-system *logical-system-name* | all | root-logical-system]

The user logical system administrator can issue the following statement:

clear security application-firewall rule-set statistics all

Release Information Command introduced in Junos OS Release 11.4.

Description Clear all security application firewall rule set statistics.

NOTE: User logical system administrators can clear statistics only for the logical systems they can access. For information about master and user administrator roles in logical systems, see *Junos OS Logical Systems Library for Security Devices*.

Options ***logical-system-name***—Name of a specific logical system.

all—(default) Clear all rule set statistics for a specific logical system or all logical systems.

root-logical-system—Clear application firewall rule set statistics on the root logical system (master administrator only).

Required Privilege Level clear

Related Documentation

- *Application Firewall Feature Guide for Security Devices*
- *show security application-firewall rule-set logical-system*

Output Fields This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

show security application-firewall rule-set

Supported Platforms SRX Series

Syntax show security application-firewall rule-set (*<rule-set-name>* | all)

Release Information Command introduced in Junos OS Release 11.1. Updated in Junos OS Release 12.1X44-D10 with output format changes. Updated in Junos OS Release 12.1X45-D10 with redirection counters.

Description Display information about the specified rule set defined in the application firewall.

Options ***rule-set-name***—Name of the rule set.

all—Display information about all the application firewall rule sets.

Required Privilege Level view

Related Documentation

- *Application Firewall Feature Guide for Security Devices*
- *clear security application-firewall rule-set statistics*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output

show security application-firewall rule-set my_ruleset1 on page 150
show security application-firewall rule-set all on page 150

Output Fields Table 14 on page 149 lists the output fields for the **show security application-firewall rule-set** command. Output fields are listed in the approximate order in which they appear.

Table 14: show security application-firewall rule-set Output Fields

Field Name	Field Description
Rule-set	Name of the rule set.
Logical system	Name of the logical system of the rule set.
Profile	The redirect profile to be used for rules requiring redirection for reject or deny actions.

Copyright © 2013, Juniper Networks, Inc.

Table 14: show security application-firewall rule-set Output Fields *(continued)*

Field Name	Field Description

Rule	Name of the rule
	• **Dynamic applications**—Name of the applications.
	• **Dynamic application groups**—Name of the application groups.
	• **SSL-Encryption**—Setting for SSL traffic.
	• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  ◦ **permit**
	  ◦ **deny**
	  ◦ **reject**
	  ◦ **redirect**
	• **Number of sessions matched**—Number of sessions matched with the application firewall rule.
	• **Number of sessions redirected**—Number of sessions redirected by the application firewall rule.

Default rule	The default rule applied when the identified application is not specified in any rules of the rule set. • **Number of sessions matched**—Number of sessions matched with the application firewall default rule. • **Number of sessions redirected**—Number of sessions redirected by the application firewall rule.
Number of sessions with appid pending	Number of sessions that are pending application identification processing

Sample Output

show security application-firewall rule-set my_ruleset1

```
user@host>show security application-firewall rule-set my_ruleset1
Rule-set: my_ruleset1
     Rule: rule1
         Dynamic Applications: junos:facebook, junos:messenger
         Dynamic Application Groups: junos:web, junos:chat
         SSL-Encryption: any
         Action: deny or redirect
         Number of sessions matched: 10
         Number of sessions redirected: 10
     Default rule: permit
         Number of sessions matched: 200
         Number of sessions redirected: 0
     Number of sessions with appid pending: 2
```

Sample Output

show security application-firewall rule-set all

```
user@host>  show security application-firewall rule-set all
Rule-set: appfw
    Logical system: root-logical-system
```


Copyright © 2013, Juniper Networks, Inc.

```
Profile: lsy2_pf555
Rule: 2
    Dynamic Applications: junos:HTTP
    SSL-Encryption: any
    Action:deny or redirect
    Number of sessions matched: 2
    Number of sessions redirected: 2
Rule: 1
    Dynamic Applications: junos:FTP
    SSL-Encryption: any
    Action:permit
    Number of sessions matched: 0
    Number of sessions redirected: 0
Default rule:permit
    Number of sessions matched: 0
    Number of sessions redirected: 0
Number of sessions with appid pending: 0
```

Copyright © 2013, Juniper Networks, Inc.

show security application-tracking counters

Supported Platforms SRX Series

Syntax show security application-tracking counters

Release Information Command introduced in Junos OS Release 10.2.

Description Display the status of AppTrack counters.

Required Privilege Level view

Related Documentation
- *Application Tracking Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Output Fields Table 15 on page 152 lists the output fields for the **show security application-tracking counters** command. Output fields are listed in the approximate order in which they appear.

Table 15: show security application-tracking counters

Field Name	Field Description
Session create messages	The number of log messages generated when a session was created.
Session close messages	The number of log messages generated when a session was closed.
Session volume updates	The number of log messages generated when an update interval was exceeded.
Failed messages	The number of messages that were not generated due to memory or session constraints.

Sample Output

show security application-tracking counters

```
user@host> show security application-tracking counters
AVT counters:                       Value
 Session create messages              0
 Session close messages               0
 Session volume updates               0
 Failed messages                      0
```


Copyright © 2013, Juniper Networks, Inc.

show security firewall-authentication history

Supported Platforms J Series, LN Series, SRX Series

Syntax **show security firewall-authentication history**
<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 security firewall authentication history information.

Options

- none—Display history of firewall authentication information.
- **node**—(Optional) For chassis cluster configurations, display all firewall authentication history on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation

- *Firewall User Authentication Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security firewall-authentication history on page 154
show security firewall-authentication history node all on page 154

Output Fields Table 16 on page 153 lists the output fields for the **show security firewall-authentication history** command. Output fields are listed in the approximate order in which they appear.

Table 16: show security firewall-authentication history Output Fields

Field Name	Field Description
Authentications	Number of authentications.
Id	Identification number.
Source IP	IP address of the authentication source.
Date	Authentication date.
Time	Authentication time.
Duration	Authentication duration.

Copyright © 2013, Juniper Networks, Inc.

Table 16: show security firewall-authentication history Output Fields *(continued)*

Field Name	Field Description
Status	Authentication status success or failure.
User	Name of the user.

Sample Output

show security firewall-authentication history

```
user@host> show security firewall-authentication history
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 211.0.0.6       2007-04-03 11:43:06 00:00:45   Success  hello
```

Sample Output

show security firewall-authentication history node all

```
user@host> show security firewall-authentication history node all
node0:
--------------------------------------------------------------------------
History of firewall authentication data:
Authentications: 2
Id Source Ip       Date       Time     Duration   Status   User
1 100.0.0.1       2008-01-04 12:00:10 0:05:49    Success  local1
2 100.0.0.1       2008-01-04 14:36:52 0:01:03    Success  local1
node1:
--------------------------------------------------------------------------
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 100.0.0.1       2008-01-04 14:59:43 1193046:06: Success local1
```


Copyright © 2013, Juniper Networks, Inc.

show security firewall-authentication users

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security firewall-authentication users
<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 firewall authentication details about all users.

Options
- none—Display details about all firewall authentication users.
- **node**—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.
  - *node-id*—Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation
- *Firewall User Authentication Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security firewall-authentication users on page 156
show security firewall-authentication users node 0 on page 156
show security firewall-authentication users node all on page 156

Output Fields Table 17 on page 155 lists the output fields for the **show security firewall-authentication users** command. Output fields are listed in the approximate order in which they appear.

Table 17: show security firewall-authentication users Output Fields

Field Name	Field Description
Total users in table	Gives count of how many entries/users the command will display.
Id	Identification number.
Source IP	IP address of the authentication source.
Src zone	User traffic received from the zone.
Dst zone	User traffic destined to the zone.

Copyright © 2013, Juniper Networks, Inc.

Table 17: show security firewall-authentication users Output Fields *(continued)*

Field Name	Field Description
Profile	Name of profile used for authentication.
Age	Idle timeout for the user.
Status	Authentication status success or failure.
User	Name of the user.

Sample Output

show security firewall-authentication users

```
user@host> show security firewall-authentication users
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           1 1111:1212/64        z1       z2       p1       0 Success  local1
```

Sample Output

show security firewall-authentication users node 0

```
user@host> show security firewall-authentication users node 0
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User

           3 100.0.0.1       z1       z2       p1           1 Success  local1
```

Sample Output

show security firewall-authentication users node all

```
user@host> show security firewall-authentication users node all
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           3 100.0.0.1       z1       z2       p1           1 Success  local1

node1:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           2 100.0.0.1       z1       z2       p1           1 Success  local1
```


Copyright © 2013, Juniper Networks, Inc.

show security flow session

Supported Platforms J Series, SRX Series

Syntax **show security flow session**
[*filter*] [**brief | extensive | summary**]

Release Information Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2. Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2.

Description Display information about all currently active security sessions on the device.

Options

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific **show** command for examples of the filtered output.

  application—Predefined application name

  application-firewall—Application firewall enabled

  application-firewall-rule-set—Application firewall enabled with the specified rule set

  application-traffic-control—Application traffic control rule set name and rule name

  destination-port—Destination port

  destination-prefix—Destination IP prefix or address

  dynamic-application—Dynamic application or nested dynamic application

  dynamic-application-group—Dynamic application or nested dynamic application group

  encrypted—Encrypted traffic

  family—Display session by family

  idp—IDP enabled sessions

  interface—Name of incoming or outgoing interface

  logical-system (all | *logical-system-name*)—Name of a specific logical system or **all** to display all logical systems

  nat—Display sessions with network address translation

  protocol—IP protocol number

  resource-manager—Resource manager

  session-identifier—Session identifier

  source-port—Source port

Copyright © 2013, Juniper Networks, Inc.

source-prefix—Source IP prefix

tunnel—Tunnel sessions

- brief | extensive | summary—Display the specified level of output.
- none—Display information about all active sessions.

Required Privilege Level view

Related Documentation

- *Flow-Based Processing Feature Guide for Security Devices*
- *Application Identification Feature Guide for Security Devices*
- *Application Firewall Feature Guide for Security Devices*
- *Application Quality of Service Feature Guide for Security Devices*
- *clear security flow session all*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output

show security flow session on page 160
show security flow session brief on page 160
show security flow session extensive on page 160
show security flow session summary on page 161

Output Fields Table 18 on page 158 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 18: show security flow session Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.

Copyright © 2013, Juniper Networks, Inc.

Table 18: show security flow session Output Fields *(continued)*

Field Name	Field Description
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.
Dynamic application	Name of the application.
Application traffic control rule-set	AppQoS rule set for this session.
Rule	AppQoS rule for this session.
Forwarding class	The AppQoS forwarding class name for this session that distinguishes the transmission priority
DSCP code point	Differentiated Services (DiffServ) code point (DSCP) value remarked by the matching rule for this session.
Loss priority	One of four priority levels set by the matching rule to control discarding a packet during periods of congestion. A high loss priority means a high probability that the packet could be dropped during a period of congestion.
Rate limiter client to server	The rate-limiter profile assigned to the client-to-server traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications.
Rate limiter server to client	The rate-limiter profile assigned to the server-to-client traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Maximum number of sessions permitted.

Copyright © 2013, Juniper Networks, Inc.

Sample Output

show security flow session

```
root> show security flow session
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC5 PIC0:

Session ID: 100000001, Status: Normal
Flag: 0x40
Policy name: p/4
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption:  Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 296
Session State: Valid
Start time: 422, Duration: 4
   In: 15.0.0.10/3000 --> 20.0.0.10/3000;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x8, Flag: 0x21
    Route: 0x0, Gateway: 15.0.0.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 104
   Out: 20.0.0.10/3000 --> 15.0.0.10/3000;tcp,
```


Copyright © 2013, Juniper Networks, Inc.

```
    Interface: ge-0/0/2.0,
    Session token: 0x9, Flag: 0x20
    Route: 0x0, Gateway: 20.0.0.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1
```

show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200
```

Copyright © 2013, Juniper Networks, Inc.

show security match-policies

Supported Platforms J Series, SRX Series

Syntax

show security match-policies
destination-ip *ip-address*
destination-port *port-number*
from-zone *zone-name*
protocol *protocol-name* | *protocol-number*
result-count *number*
source-identity *role-name*
source-ip *ip-address*
source-port *port-number*
to-zone *zone-name*

Release Information

Command introduced in Release 10.3 of Junos OS.
Command updated in Release 10.4 of Junos OS.
Command updated in Release 12.1 of Junos OS.

Description

The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, then the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are "shadowed" by the first and are never encountered by matching traffic.

NOTE: The **show security match-policies** command is applicable only to security policies; IDP policies are not supported.

Options

- **destination-ip** ***destination-ip***—Destination IP address of the traffic.
- **destination-port** ***destination-port***—Destination port number of the traffic. Range is 1 through 65,535
- **from-zone** ***from-zone***—Name or ID of the source zone of the traffic.
- **protocol** ***protocol-name*** **|** ***protocol-number***—Protocol name or numeric value of the traffic.
  - **ah** or **51**
  - **egp** or **8**
  - **esp** or **50**
  - **gre** or **47**
  - **icmp** or **1**

Copyright © 2013, Juniper Networks, Inc.

- **igmp** or **2**
- **igp** or **9**
- **ipip** or **94**
- **ipv6** or **41**
- **ospf** or **89**
- **pgm** or **113**
- **pim** or **103**
- **rdp** or **27**
- **rsvp** or **46**
- **sctp** or **132**
- **tcp** or **6**
- **udp** or **17**
- **vrrp** or **112**

- **result-count** ***number***—(Optional) The number of policy matches to display. Valid range is from 1 through 16. The default value is 1.
- **source-identity** ***role-name***—Source identity of the traffic determined by the user role.
- **source-ip** ***source-ip***—Source IP address of the traffic.
- **source-port** ***source-port***—Source port number of the traffic. Range is 1 through 65,535.
- **to-zone** ***to-zone***—Name or ID of the destination zone of the traffic.

Required Privilege Level view

Related Documentation
- *clear security policies statistics*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
Example 1: show security match-policies on page 165
Example 2: show security match policies ... result-count on page 165
Example 3: show security match policies ... source-identity on page 166

Output Fields Table 19 on page 163 lists the output fields for the **show security match-policies** command. Output fields are listed in the approximate order in which they appear.

Table 19: show security match-policies Output Fields

Field Name	Field Description
Policy:	Name of the applicable policy.

Copyright © 2013, Juniper Networks, Inc.

Table 19: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Action or **Action-type:**	The action to be taken for traffic that matches the policy's match criteria. Actions include the following: • **permit** • **firewall-authentication** • **tunnel ipsec-vpn** *vpn-name* • **pair-policy** *pair-policy-name* • **source-nat pool** *pool-name* • **pool-set** *pool-set-name* • **interface** • **destination-nat** *name* • **deny** • **reject**
State:	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index:	An internal number associated with the policy.
Sequence number:	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.
From zone:	Name of the source zone.
To zone:	Name of the destination zone.
Source addresses:	The names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses:	The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it.
Application	Name of a preconfigured or custom application, or **any** if no application is specified.
IP protocol:	Numeric value for the IP protocol used by the application, such as 6 for TCP or 1 for ICMP.
ALG:	If an ALG is associated with the session, the name of the ALG. Otherwise, 0.
Inactivity timeout:	Elapsed time without activity after which the application is terminated.
Source-port range:	Range of matching source ports defined in the policy.

Copyright © 2013, Juniper Networks, Inc.

Table 19: show security match-policies Output Fields *(continued)*

Field Name	Field Description
Destination-port range:	Range of matching destination ports defined in the policy.
Source identites	One or more user roles defined in the matching policy.

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 30.30.30.1 source-port 1 destination-port 21 protocol tcp
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 20.20.0.0/16
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 40.40.0.0/16
    d3: 30.30.30.1/32
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [21-21]
```

Example 2: show security match policies ... result-count

```
user@host> show security match-policies source-ip 10.10.10.1 destination-ip 20.20.20.5
source_port 1004 destination_port 80 protocol tcp result_count 5
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 20.20.0.0/16
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
  Sequence number: 15
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa11: 10.10.10.1/32
  Destination addresses:
    da15: 20.20.20.5/32
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]
```

Copyright © 2013, Juniper Networks, Inc.

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 20.20.20.5 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: 20.0.0.0/8
      Destination addresses:
        d1: 21.0.0.0/8
      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
```


Copyright © 2013, Juniper Networks, Inc.

show security nat destination rule

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security nat destination rule
rule-name
all
logical-system (*logical-system-name* | all)
root-logical-system

Release Information Command introduced in Junos OS Release 9.2. The **Description** output field added in Junos OS Release 12.1. Support for IPv6 logical systems and the **Successful sessions**, **Failed sessions**, and **Number of sessions** output fields added in Junos OS Release 12.1X45-D10.

Description Display information about the specified destination Network Address Translation (NAT) rule.

Options
rule-name—Display information about the specified destination NAT rule.

all—Display information about all the destination NAT rules.

logical-system (*logical-system-name* | all)—Display information about the destination NAT rules for the specified logical system or for all logical systems.

root-logical-system—Display information about the destination NAT rules for the master (root) logical system.

Required Privilege Level view

Related Documentation
- *rule (Security Destination NAT)*
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security nat destination rule dst2-rule on page 168
show security nat destination rule all on page 169

Output Fields Table 20 on page 167 lists the output fields for the **show security nat destination rule** command. Output fields are listed in the approximate order in which they appear.

Table 20: show security nat destination rule Output Fields

Field Name	Field Description
Total destination-nat rules	Number of destination NAT rules.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly as address names and as address set names in the rule.

Copyright © 2013, Juniper Networks, Inc.

Table 20: show security nat destination rule Output Fields *(continued)*

Field Name	Field Description
Destination NAT rule	Name of the destination NAT rule.
Description	Description of the destination NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the destination NAT rule.
From routing instance	Name of the routing instance from which the packets flow.
From interface	Name of the interface from which the packets flow.
From zone	Name of the zone from which the packets flow.
Source addresses	Name of the source addresses which match the rule. The default value is any.
Destination addresses	Name of the destination addresses which match the rule. The default value is any.
Action	The action taken when a packet matches the rule's tuples. Actions include the following: • **destination NAT pool**—Use user-defined destination NAT pool to perform destination NAT. • **off**—Do not perform destination NAT.
Destination port	Destination ports number which match the rule. The default value is any.
Translation hits	Number of translation hits.
Successful sessions	Number of successful session installations after the NAT rule is matched.
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat destination rule dst2-rule

```
user@host>show security nat destination rule dst2-rule

 Destination NAT rule: dst2-rule           Rule-set: dst2
  Description               : The destination rule dst2-rule is for the sales
team
  Rule-Id                   : 1
  Rule position             : 1
  From routing instance     : ri1
                            : ri2
  Match
    Source addresses        : add1
```


Copyright © 2013, Juniper Networks, Inc.

```
                                add2
    Destination addresses    : add9
  Action                     : off

  Destination port           : 0
 Translation hits            : 68
   Successful sessions       : 25
   Failed sessions           : 43
 Number of sessions          : 2
```

Sample Output

show security nat destination rule all

```
user@host> show security nat destination rule all

Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 1/0

Destination NAT rule: drule                Rule-set: drs
  Rule-Id                    : 1
  Rule position              : 1
  From zone                  : untrust
    Destination addresses    : 99.1.1.1        - 99.1.1.1

  Destination port           : 0
  Action                     : dpool1
  Translation hits           : 68
   Successful sessions       : 25
   Failed sessions           : 43
 Number of sessions          : 2
```

Copyright © 2013, Juniper Networks, Inc.

show security nat destination summary

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security nat destination summary
<logical-system (*logical-system-name* | all)>
<root-logical-system>

Release Information Command introduced in Junos OS Release 9.2. Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10.

Description Display a summary of Network Address Translation (NAT) destination pool information.

Options
none—Display summary information about the destination NAT pool.

logical-system (*logical-system-name* | all)—Display summary information about the destination NAT for the specified logical system or for all logical systems.

root-logical-system—Display summary information about the destination NAT for the master (root) logical system.

Required Privilege Level view

Related Documentation
- *pool (Security Destination NAT)*
- *rule (Security Destination NAT)*
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output show security nat destination summary on page 171

Output Fields Table 21 on page 170 lists the output fields for the **show security nat destination summary** command. Output fields are listed in the approximate order in which they appear.

Table 21: show security nat destination summary Output Fields

Field Name	Field Description
Total destination nat pool number	Number of destination NAT pools.
Pool name	Name of the destination address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
Port	Port number.
Total	Number of IP addresses that are in use.

Copyright © 2013, Juniper Networks, Inc.

Table 21: show security nat destination summary Output Fields *(continued)*

Field Name	Field Description
Available	Number of IP addresses that are free for use.
Total destination nat rule number	Number of destination NAT rules.
Total hit times	Number of times a translation in the translation table is used for all the destination NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the destination NAT rules.

Sample Output

show security nat destination summary

```
user@host> show security nat destination summary

Total pools: 2
Pool name            Address                   Routing        Port  Total
                     Range                     Instance             Address
dst-p1               1.1.1.1  - 1.1.1.1         default        0     1
dst-p2               2001::1  - 2001::1         default        0     1

Total rules: 171
Rule name            Rule set       From                            Action
dst2-rule            dst2           ri1
                                    ri2
                                    ri3
                                    ri4
                                    ri5
                                    ri6
                                    ri7
dst3-rule            dst3           ri9                             off
                                    ri1
                                    ri2
                                    ri3
                                    ri4
                                    ri5

...
```

Copyright © 2013, Juniper Networks, Inc.

show security nat source rule

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security nat source rule
rule-name
all
logical-system (*logical-system-name* | all)
root-logical-system

Release Information Command introduced in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 11.2. The **Description** output field added in Junos OS Release 12.1. Support for IPv6 logical systems and the **Source port**, **Successful sessions**, **Failed sessions**, and **Number of sessions** output fields added in Junos OS Release 12.1X45-D10.

Description Display information about the specified source Network Address Translation (NAT) rule.

Options
rule-name—Name of the rule.

all—Display information about all the source NAT rules.

logical-system (*logical-system-name* | all)—Display information about the source NAT rules for the specified logical system or for all logical systems source NAT rules.

root-logical-system—Display information about the source NAT rules for the master (root) logical system.

Required Privilege Level view

Related Documentation
- *rule (Security Source NAT)*
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security nat source rule r2 on page 174
show security nat source rule all on page 174

Output Fields Table 22 on page 172 lists the output fields for the **show security nat source rule** command. Output fields are listed in the approximate order in which they appear

Table 22: show security nat source rule Output Fields

Field Name	Field Description
Source NAT rule	Name of the source NAT rule.
Total rules	Number of source NAT rules.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule.

Copyright © 2013, Juniper Networks, Inc.

Table 22: show security nat source rule Output Fields *(continued)*

Field Name	Field Description
Description	Description of the source NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the source NAT rule.
From zone	Name of the zone from which the packets flow.
To zone	Name of the zone to which the packets flow.
From routing instance	Name of the routing instance from which the packets flow.
To routing instance	Name of the routing instance to which the packets flow.
From interface	Name of the interface from which the packets flow.
To interface	Name of the interface to which the packets flow.
Source addresses	Name of the source addresses that match the rule.
Source port	Source port numbers that match the rule.
Destination address	Name of the destination addresses that match the rule.
Destination port	Destination port numbers that match the rule.
Action	The action taken in regard to a packet that matches the rule's tuples. Actions include the following: • **off**—Do not perform source NAT. • **source NAT pool**—Use user-defined source NAT pool to perform source NAT • **interface**—Use egress interface's IP address to perform source NAT.
Persistent NAT type	Persistent NAT type.
Persistent NAT mapping type	Persistent NAT mapping type.
Inactivity timeout	Inactivity timeout for persistent NAT binding.
Max session number	Maximum number of sessions.
Translation hits	Number of translation hits.
Successful sessions	Number of successful session installations after the NAT rule is matched.
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.

Copyright © 2013, Juniper Networks, Inc.

Table 22: show security nat source rule Output Fields *(continued)*

Field Name	Field Description
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat source rule r2

```
user@host> show security nat source rule r2

 source NAT rule: r2        Rule-set: src-nat
  Description               : The source rule r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone1
  To zone                   : zone9
  Match
   Source addresses         : add1
                              add2
   Destination addresses    : add9
                              add10
   Destination port         : 1002            - 1002
  Action                       : off
    Persistent NAT type        : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout         : 0
    Max session number         : 0
  Translation hits             : 4719
   Successful sessions       : 2000
   Failed sessions           : 2719
 Number of sessions          : 5
```

Sample Output

show security nat source rule all

```
user@host> show security nat source rule all
Logical system: root

Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 3/0

source NAT rule: srule               Rule-set: srs
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : trust
  To zone                   : untrust
  Match
    Source addresses        : 10.10.10.0      - 10.10.10.255
    Destination addresses   : 20.20.20.0      - 20.20.20.255
                              30.30.30.0      - 30.30.30.255
    Source port             : 100             - 200
                              500             - 500
  Action                      : sp1
    Persistent NAT type       : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout        : 0
```


Copyright © 2013, Juniper Networks, Inc.

```
  Max session number          : 0
Translation hits             : 4719
 Successful sessions         : 2000
 Failed sessions             : 2719
Number of sessions           : 5
```

Copyright © 2013, Juniper Networks, Inc.

show security nat source summary

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security nat source summary
<logical-system (*logical-system-name* | all)>
<root-logical-system>

Release Information Command introduced in Junos OS Release 9.2. Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10.

Description Display a summary of Network Address Translation (NAT) source information.

Options
none—Display summary source NAT information.

logical-system (*logical-system-name* | all)—Display summary information about the source NAT for the specified logical system or for all logical systems.

root-logical-system—Display summary information about the source NAT for the master (root) logical system.

Required Privilege Level view

Related Documentation
- *pool (Security Source NAT)*
- *rule (Security Source NAT)*
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output show security nat source summary on page 177

Output Fields Table 23 on page 176 lists the output fields for the **show security nat source summary** command. Output fields are listed in the approximate order in which they appear.

Table 23: show security nat source summary Output Fields

Field Name	Field Description
Total source nat pool number	Number of source NAT pools.
Pool name	Name of the source address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
PAT	Whether Port Address Translation (PAT) is enabled (yes or no).
Total Address	Number of IP addresses that are in use.

Copyright © 2013, Juniper Networks, Inc.

Table 23: show security nat source summary Output Fields *(continued)*

Field Name	Field Description
Total source nat rule number	Number of source NAT rules.

Sample Output

show security nat source summary

```
root@host> show security nat source summary logical-system all


Logical system: root-logical-system
Total port number usage for port translation pool: 67108864
Maximum port number for port translation pool: 134217728

Logical system: lsys1
Total port number usage for port translation pool: 193536
Maximum port number for port translation pool: 134217728
Total pools: 2

Logical system: root-logical-system
Pool              Address                   Routing   PAT   Total
Name              Range                     Instance        Address
pool1             1.1.1.0-1.1.4.255-        default   yes   2048
                  1.1.5.0-1.1.8.255


Logical system: lsys1
Pool              Address                    Routing   PAT   Total
Name              Range                      Instance        Address
pool2             30.1.1.1-30.1.1.3          default   yes   3


Total rules: 1

Logical system: root-logical-system
Rule name         Rule set      From         To             Action
rule 1            ruleset1      ge-2/2/2.0   ge-2/2/3.0     pool1
rule 1                          ge-2/2/4.0   ge-2/2/5.0
```

Copyright © 2013, Juniper Networks, Inc.

show security nat static rule

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security nat static rule
rule-name
all
logical-system (*logical-system-name* | all)
root-logical-system

Release Information Command introduced in Junos OS Release 9.3. The **Description** output field added in Junos OS Release 12.1. Support for IPv6 logical systems and the **Successful sessions**, **Failed sessions**, **Number of sessions**, **Source addresses,** and **Source ports** output fields added in Junos OS Release 12.1X45-D10.

Description Display information about the specified static Network Address Translation (NAT) rule.

Options
rule-name—Name of the rule.

all—Display information about all the static NAT rules.

logical-system (*logical-system-name* | all)—Display information about the static NAT rules for the specified logical system or for all logical systems.

root-logical-system—Display information about the static NAT rules for the master (root) logical system.

Required Privilege Level view

Related Documentation
- *rule (Security Static NAT)*
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security nat static rule sta-r2 on page 179
show security nat static rule all on page 180

Output Fields Table 24 on page 178 lists the output fields for the **show security nat static rule** command. Output fields are listed in the approximate order in which they appear.

Table 24: show security nat static rule Output Fields

Field Name	Field Description
Static NAT rule	Name of the static NAT rule.
Total referenced IPv4/IPv6 ip-prefixes	Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule.
Rule-set	Name of the rule set. Currently, you can configure 8 rules within the same rule set.

Copyright © 2013, Juniper Networks, Inc.

Table 24: show security nat static rule Output Fields *(continued)*

Field Name	Field Description
Description	Description of the static NAT rule.
Rule-Id	Rule identification number.
Rule position	Position of the rule that indicates the order in which it applies to traffic.
From interface	Name of the interface from which the packets flow.
From routing instance	Name of the routing instance from which the packets flow.
From zone	Name of the zone from which the packets flow.
Destination addresses	Name of the destination addresses that match the rule.
Source addresses	Name of the source addresses that match the rule.
Host addresses	Name of the host addresses that match the rule.
Netmask	Subnet IP address.
Host routing-instance	Name of the host routing instance.
Destination port	Destination port numbers that match the rule. The default value is any.
Source port	Source port numbers that match the rule.
Total static-nat rules	Number of static NAT rules.
Translation hits	Number of times a translation in the translation table is used for a static NAT rule.
Successful sessions	Number of successful session installations after the NAT rule is matched.
Failed sessions	Number of unsuccessful session installations after the NAT rule is matched.
Number of sessions	Number of sessions that reference the specified rule.

Sample Output

show security nat static rule sta-r2

```
user@host> show security nat static rule sta-r2

 Static NAT rule: sta-r2                 Rule-set: sta-nat
  Description               : The static rule sta-r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone9
  Destination addresses     : add3
```

Copyright © 2013, Juniper Networks, Inc.

```
  Host addresses             : add4
  Netmask                    : 24
  Host routing-instance      : N/A
  Translation hits           : 2
   Successful sessions      : 2
   Failed sessions          : 0
 Number of sessions         : 2
```

Sample Output

show security nat static rule all

```
user@host> show security nat static rule all

Static NAT rule: r1                   Rule-set: rs1
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : trust
  Source addresses          : 40.10.10.0 - 40.10.10.3
                            : addr1
  Source ports              : 200 - 300
  Destination addresses     : 20.1.1.0
  Host addresses            : 3.3.3.0
  Netmask                   : 24
  Host routing-instance     : N/A
  Translation hits          : 4
   Successful sessions      : 4
   Failed sessions          : 0
 Number of sessions         : 4
Static NAT rule: r2                   Rule-set: rs1
  Rule-Id                   : 2
  Rule position             : 2
  From zone                 : trust
  Source addresses          : 40.10.10.0 - 40.10.10.255
  Destination addresses     : 30.1.1.1
  Destination ports         : 100 - 200
  Host addresses            : 40.1.1.1
  Host ports                : 300 - 400
  Netmask                   : 32
  Host routing-instance     : N/A
  Translation hits          : 4
   Successful sessions      : 4
   Failed sessions          : 0
 Number of sessions         : 4
```


Copyright © 2013, Juniper Networks, Inc.

show security policies

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security policies
<detail>
<none>
policy-name *policy-name*
<detail>
<global>

Release Information Command modified in Junos OS Release 9.2. 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 global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The **Description** output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10.

Description Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.

Options
- **none**—Display basic information about all configured policies.
- **detail**—(Optional) Display a detailed view of all of the policies configured on the device.
- **policy-name *policy-name***—(Optional) Display information about the specified policy.
- **global**—Display information about global policies.

Required Privilege Level view

Related Documentation
- *Ethernet Port Switching Feature Guide for Security Devices*
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*
- *Junos OS UTM Library for Security Devices*
- *Security Policies Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output

Copyright © 2013, Juniper Networks, Inc.

Output Fields Table 25 on page 182 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 25: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
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	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.
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 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.

Copyright © 2013, Juniper Networks, Inc.

Table 25: show security policies Output Fields *(continued)*

Field Name	Field Description
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The IP protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is 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.
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 in regard to a packet that matches the policy's tuples. Actions include the following: ◦ **permit** ◦ **firewall-authentication** ◦ **tunnel ipsec-vpn** *vpn-name* ◦ **pair-policy** *pair-policy-name* ◦ **source-nat pool** *pool-name* ◦ **pool-set** *pool-set-name* ◦ **interface** ◦ **destination-nat** *name* ◦ **deny** ◦ **reject** ◦ **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.

Copyright © 2013, Juniper Networks, Inc.

Table 25: show security policies Output Fields *(continued)*

Field Name	Field Description
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active (or inactive) to check an incoming packet to determine how to treat the packet.
Policy statistics	Policy statistics include the following: • **Input bytes**—The number of bytes presented for processing by the device. • **Output bytes**—The number of bytes actually processed by the device. • **Input packets**—The number of packets presented for processing by the device. • **Active sessions**—The number of sessions currently present because of access control lookups that used this policy. • **Session deletions**—The number of sessions deleted since system startup. • **Policy lookups**—Number of times the policy was accessed to check for a match. NOTE: Configure the Policy P1 with the **count** option to display policy statistics.

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: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
    Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
    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: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    Source identities: role1, role4
    Applications: any
    Action: deny, scheduled
```

show security policies policy-name p1 detail

```
user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
  Description: The policy p1 is for the sales team
```


Copyright © 2013, Juniper Networks, Inc.

```
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
  Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
 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, junos:YSMG
      Dynamic Application groups: junos:web, junos:chat
      Action: deny
    Default rule: permit
  Session log: at-create, at-close
  Scheduler name: sch20
  Policy statistics:
    Input  bytes     :                50000                 100 bps
    Output bytes     :                40000                 100 bps
    Input  packets   :                  200                 200 pps
    Output packets   :                  100                 100 pps
    Session rate     :                    2                   1 sps
    Active sessions  :                   11
    Session deletions:                   20
    Policy lookups   :                   12
```

show security policies (services-offload)

```
user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload
```

Copyright © 2013, Juniper Networks, Inc.

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     :                 500                   0 bps
    Output bytes     :                 408                   0 bps
    Input  packets   :                   8                   0 pps
    Output packets   :                   6                   0 pps
    Session rate     :                   3                   0 sps
    Active sessions  :                   1
    Session deletions:                   2
    Policy lookups   :                   3
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
```

show security policies policy-name p1 (Negated Address)

```
user@host>show security policies policy-name p1
node0:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

```
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 p1 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): 1.1.1.1/32
    ad3(ad): 15.100.199.56 ~ 15.200.100.16
    ad4(ad): 15.100.196.0/22
    ad5(ad): 15.1.7.199 ~ 15.1.8.19
    ad6(ad): 15.1.8.0/21
    ad7(ad): 15.1.7.0/24
  Destination addresses(excluded):
    ad13(ad2): 20.1.7.0/24
    ad12(ad2): 20.1.4.1/32
    ad11(ad2): 20.1.7.199 ~ 20.1.8.19
    ad10(ad2): 50.1.4.0/22
    ad9(ad2): 20.1.1.11 ~ 50.1.5.199
    ad8(ad2): 2.1.1.1/32
  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
```

Copyright © 2013, Juniper Networks, Inc.

show security screen statistics

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security screen statistics (zone *zone-name* | interface *interface-name*)
<logical-system (*logical-system-name* | all)>
<node (*node-id* | all | local | primary)>
<root-logical-system>

Release Information Command introduced in Release 8.5 of Junos OS. **node** options added in Release 9.0 of Junos OS. **logical-system all** option added in Junos OS Release 11.2R6. Support for IPv6 extension header screens added in Junos OS Release 12.1X46-D10.

Description Display intrusion detection service (IDS) security screen statistics.

Options

- **zone** *zone-name* —Display screen statistics for this security zone.
- **interface** *interface-name*—Display screen statistics for this interface.
- **logical-system**—(Optional) Display screen statistics for configured logical systems.
  - ***logical-system-name***—Display screen statistics for the named logical system.
  - **all**—Display screen statistics for all logical systems, including the master (root) logical system.
- **node**—(Optional) For chassis cluster configurations, display screen statistics on a specific node.
  - ***node-id***—Identification number of a 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.
- **root-logical-system**—(Optional) Display screen statistics for the master logical system only.

Required Privilege Level view

Related Documentation

- *clear security screen statistics*
- *clear security screen statistics interface*
- *clear security screen statistics zone*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security screen statistics zone scrzone on page 191
show security screen statistics zone untrust (IPv6) on page 191
show security screen statistics interface ge-0/0/3 on page 192
show security screen statistics interface ge-0/0/1 (IPv6) on page 192

Copyright © 2013, Juniper Networks, Inc.

show security screen statistics interface ge-0/0/1 node primary on page 193
show security screen statistics zone trust logical-system all on page 193

Output Fields Table 26 on page 189 lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Table 26: show security screen statistics Output Fields

Field Name	Field Description
ICMP flood	Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP flood	User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP port scan	Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP address sweep	Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.
IP tear drop	Number of teardrop attacks. Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN flood	Number of TCP SYN attacks.
IP spoofing	Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP ping of death	ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP source route option	Number of IP source route attacks.
TCP address sweep	Number of TCP address sweeps.
TCP land attack	Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN fragment	Number of TCP SYN fragments.
TCP no flag	Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set.
IP unknown protocol	Number of IPs.
IP bad options	Number of invalid options.

Copyright © 2013, Juniper Networks, Inc.

Table 26: show security screen statistics Output Fields *(continued)*

Field Name	Field Description
IP record route option	Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels.
IP timestamp option	Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP security option	Number of IP security option attacks.
IP loose source route option	Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination.
IP strict source route option	Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination.
IP stream option	Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP fragment	Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP large packet	Number of large ICMP packets.
TCP SYN FIN	Number of TCP SYN FIN packets.
TCP FIN no ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.
Source session limit	Number of concurrent sessions that can be initiated from a source IP address.
TCP SYN-ACK-ACK proxy	Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, J Series and SRX Series devices running Junos OS reject further connection requests from that IP address.
IP block fragment	Number of IP block fragments.
Destination session limit	Number of concurrent sessions that can be directed to a single destination IP address.
UDP address sweep	Number of UDP address sweeps.
IPv6 extension header	Number of packets filtered for the defined IPv6 extension headers.
IPv6 extension hop by hop option	Number of packets filtered for the defined IPv6 hop-by-hop option types.
IPv6 extension destination option	Number of packets filtered for the defined IPv6 destination option types.
IPv6 extension header limit	Number of packets filtered for crossing the defined IPv6 extension header limit.

Copyright © 2013, Juniper Networks, Inc.

Table 26: show security screen statistics Output Fields *(continued)*

IPv6 malformed header	Number of IPv6 malformed headers defined for the intrusion detection service (IDS).
ICMPv6 malformed packet	Number of ICMPv6 malformed packets defined for the IDS options.

Sample Output

show security screen statistics zone scrzone

```
user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                              Statistics
  ICMP flood                                 0
  UDP flood                                  0
  TCP winnuke                                0
  TCP port scan                              91
  ICMP address sweep                         0
  TCP sweep                                  0
  UDP sweep                                  0
  IP tear drop                               0
  TCP SYN flood                              0
  IP spoofing                                0
  ICMP ping of death                         0
  IP source route option                     0
  TCP land attack                            0
  TCP SYN fragment                           0
  TCP no flag                                0
  IP unknown protocol                        0
  IP bad options                             0
  IP record route option                     0
  IP timestamp option                        0
  IP security option                         0
  IP loose source route option               0
  IP strict source route option              0
  IP stream option                           0
  ICMP fragment                              0
  ICMP large packet                          0
  TCP SYN FIN                                0
  TCP FIN no ACK                             0
  Source session limit                       0
  TCP SYN-ACK-ACK proxy                      0
  IP block fragment                          0
  Destination session limit                  0
```

Sample Output

show security screen statistics zone untrust (IPv6)

```
user@host>show security screen statistics zone untrust
Screen statistics:

IDS attack type                           Statistics
  ICMP flood                                   0
  UDP  flood                                   0
  TCP  winnuke                                 0
  ……
  IPv6   extension header                       0
  IPv6   extension hop by hop option            0
```

Copyright © 2013, Juniper Networks, Inc.

```
  IPv6   extension destination option           0
  IPv6   extension header limit                 0
  IPv6   malformed header                       0
  ICMPv6 malformed packet                       0
```

Sample Output

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type                                 Statistics
  ICMP flood                                    0
  UDP flood                                     0
  TCP winnuke                                   0
  TCP port scan                                 91
  ICMP address sweep                            0
  TCP sweep                                     0
  UDP sweep                                     0
  IP tear drop                                  0
  TCP SYN flood                                 0
  IP spoofing                                   0
  ICMP ping of death                            0
  IP source route option                        0
  TCP land attack                               0
  TCP SYN fragment                              0
  TCP no flag                                   0
  IP unknown protocol                           0
  IP bad options                                0
  IP record route option                        0
  IP timestamp option                           0
  IP security option                            0
  IP loose source route option                  0
  IP strict source route option                 0
  IP stream option                              0
  ICMP fragment                                 0
  ICMP large packet                             0
  TCP SYN FIN                                   0
  TCP FIN no ACK                                0
  Source session limit                          0
  TCP SYN-ACK-ACK proxy                         0
  IP block fragment                             0
  Destination session limit                     0
```

Sample Output

show security screen statistics interface ge-0/0/1 (IPv6)

```
user@host> show security screen statistics interface ge-0/0/1

Screen statistics:

IDS attack type                                 Statistics
  ICMP flood                                        0
  UDP flood                                         0
  ……
  IPv6 extension header                             0
  IPv6 extension hop by hop option                  0
  IPv6 extension destination option                 0
  IPv6 extension header limit                       0
```


Copyright © 2013, Juniper Networks, Inc.

```
  IPv6 malformed header                          0
  ICMPv6 malformed packet                        0
```

Sample Output

show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
--------------------------------------------------------------------------
Screen statistics:
IDS attack type                                Statistics
  ICMP flood                                   1
  UDP flood                                    1
  TCP winnuke                                  1
  TCP port scan                                1
  ICMP address sweep                           1
  TCP sweep                                    1
  UDP sweep                                    1
  IP tear drop                                 1
  TCP SYN flood                                1
  IP spoofing                                  1
  ICMP ping of death                           1
  IP source route option                       1
  TCP land attack                              1
  TCP SYN fragment                             1
  TCP no flag                                  1
  IP unknown protocol                          1
  IP bad options                               1
  IP record route option                       1
  IP timestamp option                          1
  IP security option                           1
  IP loose source route option                 1
  IP strict source route option                1
  IP stream option                             1
  ICMP fragment                                1
  ICMP large packet                            1
  TCP SYN FIN                                  1
  TCP FIN no ACK                               1
  Source session limit                         1
  TCP SYN-ACK-ACK proxy                        1
  IP block fragment                            1
  Destination session limit                    1
```

Sample Output

show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:

IDS attack type                                Statistics
  ICMP flood                                   0
  UDP flood                                    0
  TCP winnuke                                  0
  TCP port scan                                0
  ICMP address sweep                           0
  TCP sweep                                    0
  UDP sweep                                    0
  IP tear drop                                 0
```

```
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0

Logical system: ls1
Screen statistics:

IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          0
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0

Logical system: ls2
```


Copyright © 2013, Juniper Networks, Inc.

```
Screen statistics:

IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          0
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0
```

Copyright © 2013, Juniper Networks, Inc.

show security softwires

Supported Platforms LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Syntax show security softwires <softwire-name *softwire-name*>
<logical-system (all | *logical-system-name*)>

Release Information Command introduced in Release 10.4 of Junos OS. The **logical-system** option introduced in Release 12.1 of Junos OS.

Description Display a summary of information of all the softwire concentrators and details on concentrators with specified name.

Options **softwire-name *softwire-name***—Display the details of the specified softwire concentrator.

logical-system (all | *logical-system-name*)—Display softwire information for all logical systems or for a specified logical system. This option is only available to the master administrator.

Required Privilege Level view

Related Documentation
- *Flow-Based Processing Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

Sample Output

```
user@host> show security softwires
Softwire Name            SC Address         Status   Number of SI connected
  SC-CSSI-1                 3001::1          Connected      2
  SC-CSSI-str00             3100::1          Active         0
  SC-CSSI-str01             3101::1          Inactive       0
  SC-CSSI-str02             3001::1          Connected      2520
```

```
user@host> show security softwires softwire-name SC-CSSI-1
Name of softwire: SC-CSSI-1
   SC status: Connected
   SC address: 3001::1
   Zone: trust
   VR ID: 0
 SI Address               SI Status                  SPU
 3001::2                  Active                     spu-1
 3001::2                  Active                     spu-21
 SI number: 2
```

```
user@host> show security softwires logical-system ls-product-design
Softwire Name            SC Address         Status   Number of SI connected
  sc_1                      3000::1         Connected      1
```


Copyright © 2013, Juniper Networks, Inc.

show security zones

Supported Platforms J Series, LN Series, SRX Series

Syntax
show security zones
<detail | terse>
< *zone-name* >

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.

Options
- none—Display information about all zones.
- **detail | terse**—(Optional) Display the specified level of output.
- ***zone-name*** —(Optional) Display information about the specified zone.

Required Privilege Level view

Related Documentation
- *Ethernet Port Switching Feature Guide for Security Devices*
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
- *security-zone*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show security zones on page 198
show security zones abc on page 198
show security zones abc detail on page 198
show security zones terse on page 199

Output Fields Table 27 on page 197 lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

Table 27: show security zones Output Fields

Field Name	Field Description
Security zone	Name of the security zone.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.

Copyright © 2013, Juniper Networks, Inc.

Table 27: show security zones Output Fields *(continued)*

Field Name	Field Description
Zone	Name of the zone.
Type	Type of the zone.

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
```

Sample Output

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
```

Sample Output

show security zones abc detail

```
user@host> show security zones abc detail
```


Copyright © 2013, Juniper Networks, Inc.

```
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
```

Sample Output

show security zones terse

```
user@host> show security zones terse
Zone                     Type
my-internal              Security
my-external              Security
dmz                      Security
```

show system security-profile

Supported Platforms SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Syntax show system security-profile (all-resource | *resource*) <detail | terse> <logical-system (all | *logical-system-name*)> <root-logical-system> <summary>

Release Information Command introduced in Release 11.2 of Junos OS. Support for application firewall added in Release 11.3 of Junos OS. Option to display all resources for a logical system added in Release 11.3 of Junos OS. Resource information for ports in source NAT pools with port translation added in Release 11.4 of Junos OS.

Description Display information about a resource allocated to the logical system in a security profile. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

This command can be used by the master administrator to display resource information for the master logical system or user logical system. This command can also be used by the user logical system administrator to display resource information for a user logical system.

Options Either specify **all-resource** to display information about all resources allocated for the logical system, or specify one of the following resources:

- address-book—Address books.
- appfw-rule-set—Application firewall rule set entries.
- appfw-rule—Application firewall rule entries.
- auth-entry—Firewall authentication entries.
- cpu—CPU utilization.
- flow-gate—Flow gates, also known as pinholes.
- flow-session—Flow sessions.
- nat-cone-binding—Network Address Translation (NAT) cone bindings.
- nat-destination-pool—NAT destination pools.
- nat-destination-rule—NAT destination rules.
- nat-nopat-address—NAT without port address translations.
- nat-pat-address—NAT with port address translations.
- nat-pat-portnum—NAT source port numbers for port translation
- nat-port-ol-ipnumber—NAT port overloading IP numbers.
- nat-rule-referenced-prefix—NAT rule referenced IP-prefixes.
- nat-source-pool—NAT source pools.
- nat-source-rule—NAT source rules.

Copyright © 2013, Juniper Networks, Inc.

- nat-static-rule—NAT static rules.
- policy—Security policies.
- policy-with-count—Security policies with a count.
- scheduler—Schedulers.
- zone—Security zones.

detail | terse—(Optional) Display the specified level of output.

The following options are available only to the master administrator:

- logical-system—Display resource information for a specified user logical system. Specify **all** to display resource information for all logical systems, including the master logical system.
- root-logical-system—Display resource information for the master (root) logical system.
- summary—Display summary information about the resource for all logical systems.

Required Privilege Level view

Related Documentation
- *security-profile-resources* configuration statement
- *Junos OS Logical Systems Library for Security Devices*

List of Sample Output
show system security-profile all-resource on page 202
show system security-profile policy on page 202
show system security-profile cpu on page 202
show system security-profile cpu logical-system all on page 203
show system security-profile cpu summary on page 203
show system security-profile nat-pat-portnum on page 203
show system security-profile nat-pat-portnum summary on page 204

Output Fields Table 28 on page 201 lists the output fields for the **show system security-profile** command. Output fields are listed in the approximate order in which they appear.

Table 28: show system security-profile Output Fields

Field Name	Field Description
logical system name	Name of the logical system.
security profile name	Name of the security profile bound to the logical system.
usage	Number of resources that are currently being used by the logical system.
reserved	Number of resources that are guaranteed to be available to the logical system.
maximum	Number of resources that the logical system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources.

Copyright © 2013, Juniper Networks, Inc.

Table 28: show system security-profile Output Fields *(continued)*

Field Name	Field Description
CPU control	**TRUE** if CPU control is enabled or **FALSE** if CPU control is not enabled.
CPU control target	Upper limit for CPU utilization on the device. The default value is 80 percent.
CPU name	Central point (CP) or services processing unit (SPU). CP utilization and average utilization of all SPUs is shown. The **detail** option shows CPU utilization on each SPU.
drop rate	Packets dropped for CPU control.

Sample Output

show system security-profile all-resource

```
user@host> show system security-profile all-resource

resource                                  usage    reserved     maximum

[logical system name:   root-logical-system]
[security profile name: Default-Profile]
address-book                                  0           0         512
auth-entry                                    0           0  2147483647
cpu on CP                                 0.00%       1.00%      80.00%
cpu on SPU                                0.00%       1.00%      80.00%
flow-gate                                     0           0      524288
flow-session                                  2           0     6291456
nat-cone-binding                              0           0       65536
nat-destination-pool                          0           0        4096
nat-destination-rule                          0           0        8192
nat-nopat-address                             0           0     1048576
nat-pat-address                               0           0        2048
nat-port-ol-ipnumber                          0           0           4
nat-rule-referenced-prefix                    0           0     1048576
nat-source-pool                               0           0        2048
nat-source-rule                               0           0        8192
nat-static-rule                               0           0       20480
policy                                        0           0       40000
policy-with-count                             0           0        1024
scheduler                                     0           0          64
zone                                          0           0         512
```

show system security-profile policy

```
user@host> show system security-profile policy
logical system name   security profile name       usage    reserved     maximum

ls-product-design     ls-design-profile               0          40          50
```

show system security-profile cpu

```
user@host> show system security-profile cpu
CPU control: TRUE
CPU control target: 80.00%
logical system name    profile name    CPU name    usage(%)    reserved(%)
drop rate(%)
```


Copyright © 2013, Juniper Networks, Inc.

```
root-logical-system    Default-Profile CP            0.00%          1.00%
     0.00%
root-logical-system    Default-Profile SPU           0.00%          1.00%
     0.00%
```

show system security-profile cpu logical-system all

```
user@host> show system security-profile cpu logical-system all
CPU control: TRUE
CPU control target: 80.00%
logical system name    profile name    CPU name    usage(%)    reserved(%)
drop rate(%)
root-logical-system    Default-Profile CP            0.00%          1.00%
     0.00%
root-logical-system    Default-Profile SPU           0.00%          1.00%
     0.00%
ls-product-design      ls-design-profile CP          0.00%          0.00%
     0.00%
ls-product-design      ls-design-profile SPU         0.00%          0.00%
     0.00%
ls-marketing-dept      ls-acct-mrkt-profile CP       0.00%          0.00%
     0.00%
ls-marketing-dept      ls-acct-mrkt-profile SPU      0.00%          0.00%
     0.00%
```

Should the above output actually look as follows?

```
logical system name    security profile name    usage    reserved    maximum
root-logical-system    Default-Profile         67108864     0      134217728
lsys1                  profile1                193536     6000     134217728
```

show system security-profile cpu summary

```
user@host> show system security-profile cpu summary
CPU control: TRUE
CPU control target: 80.00%

CPU type                :     CP
global used amount      :  0.00%
global maximum quota    : 80.00%
global available amount : 80.00%
total logical systems   :      3
total security profiles :      3
heaviest usage / user   :  0.00%      / root-logical-system
lightest usage / user   :  0.00%      / root-logical-system

CPU type                :    SPU
global used amount      :  0.00%
global maximum quota    : 80.00%
global available amount : 80.00%
total logical systems   :      3
total security profiles :      3
heaviest usage / user   :  0.00%      / root-logical-system
lightest usage / user   :  0.00%      / root-logical-system
```

show system security-profile nat-pat-portnum

```
user@host> show system security-profile cpu nat-pat-portnum
CPU control: TRUE
CPU control target: 80.00%
logical system name    security profile name        usage(%)    reserved(%)
maximum
```

Copyright © 2013, Juniper Networks, Inc.

```
root-logical-system    Default-Profile CP             67108864          0
    134217728
```

show system security-profile nat-pat-portnum summary

```
user@host> show system security-profile nat-pat-portnum summary
global used amount    :67302400
global maximum quota    :134217728
global available amount   :66915328
total logical systems    :2
total security profiles   :1
heaviest usage / user    :193536 / lsys1
```


Copyright © 2013, Juniper Networks, Inc.

PART 4

Index

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

Index

Symbols

A

B

C

D

F

I

L

M

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.