JUNIPER NETWORKS

Junos® OS

Logical Systems Configuration Guide for Security Devices

Release
12.1

Published: 2012-03-06

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

Junos OS Logical Systems Configuration Guide for Security Devices
Release 12.1

Revision History
March 2012—R1 Junos OS 12.1

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

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

About This Guide

This preface provides the following guidelines for using the *Junos OS Logical Systems Configuration Guide for Security Devices*.

SRX Series Documentation and Release Notes

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

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

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

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

Objectives

This guide provides an overview of the logical systems features and explains how to configure them.

Audience

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

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

NOTE: For information about configuring logical systems on Juniper Networks M Series, MX Series, and T Series routers, see the *Junos OS Logical Systems Configuration Guide*.

Supported Routing Platforms

This manual describes features supported on the SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways running Junos OS.

Documentation Conventions

Table 1 on page viii 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 ix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

J-Web GUI Conventions

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

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

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/

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

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

Opening a Case with JTAC

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

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

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

PART 1

Part 1 Introduction

CHAPTER 1

Logical Systems Overview

Understanding Logical Systems for SRX Series Services Gateways

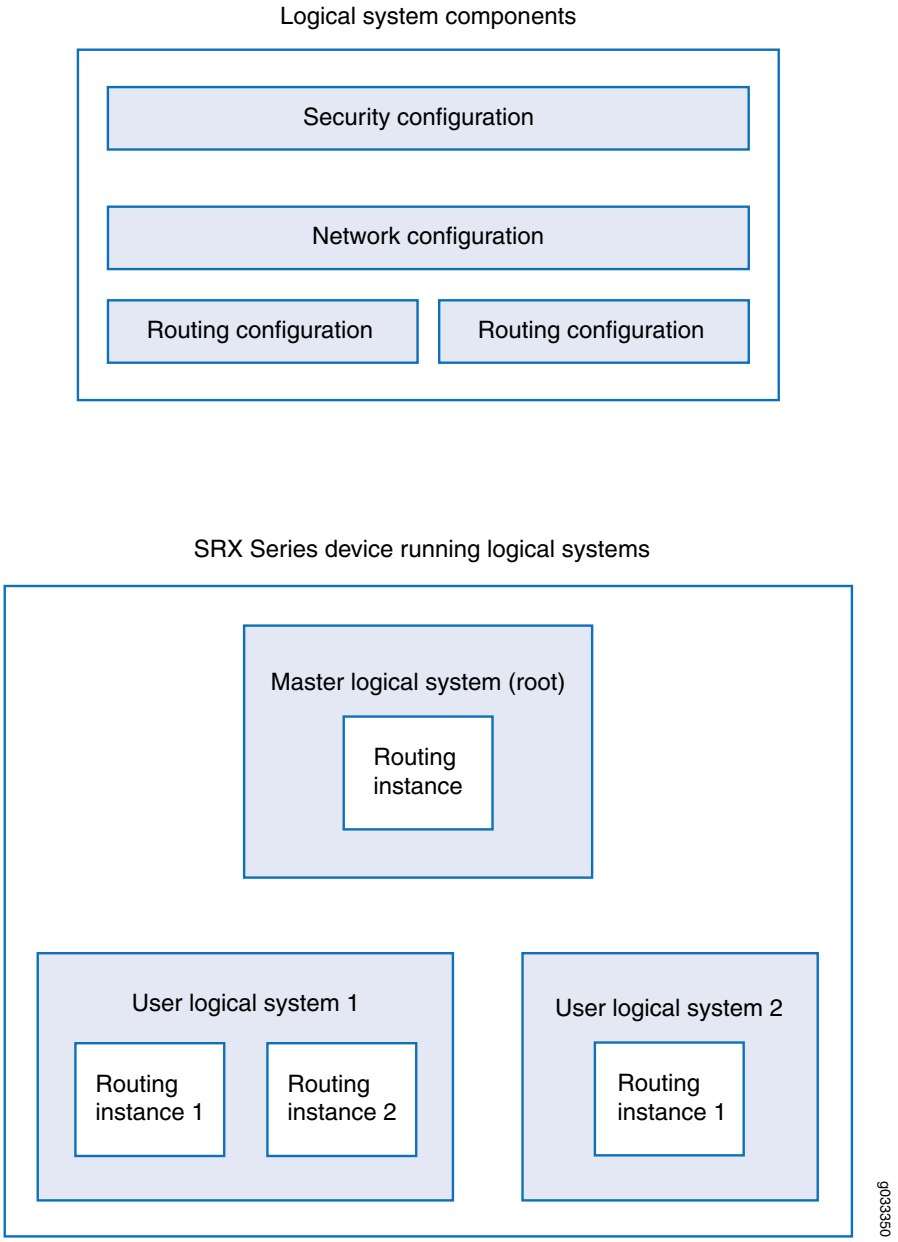
Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming an SRX Series device into a multitenant 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.

NOTE: For information about configuring logical systems on Juniper Networks M Series, MX Series, and T Series routers, see the *Junos OS Logical Systems Configuration Guide*.

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.

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Understanding the Fundamentals and Constraints of Logical Systems

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.

- 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Understanding Licenses for Logical Systems on SRX Series Devices

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 *Junos OS Installation and Upgrade Guide*.

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.

The best and safest approach to configuring logical systems and licenses is to configure only as many logical systems as you have licenses for. 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 commit additional logical systems. However, when you attempt to commit their configurations, the system issues a warning message similar to the following, telling you the number of logical systems without licenses.

NOTE: **"Warning: 2 more license(s) are needed, logical system won't work without license!"**

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
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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Understanding the Master Logical System and the Master Administrator Role

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.

  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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9
- 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 User Logical Systems on page 47

Understanding User Logical Systems and the User Logical System Administrator Role

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- 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 User Logical Systems on page 47
- Understanding Logical Systems Security Profiles on page 34
- Example: Configuring Logical Systems Security Profiles on page 40

Understanding the Interconnect Logical System and Logical Tunnel Interfaces

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 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for User Logical Systems on page 47
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Understanding Logical Systems in the Context of Chassis Cluster on page 157

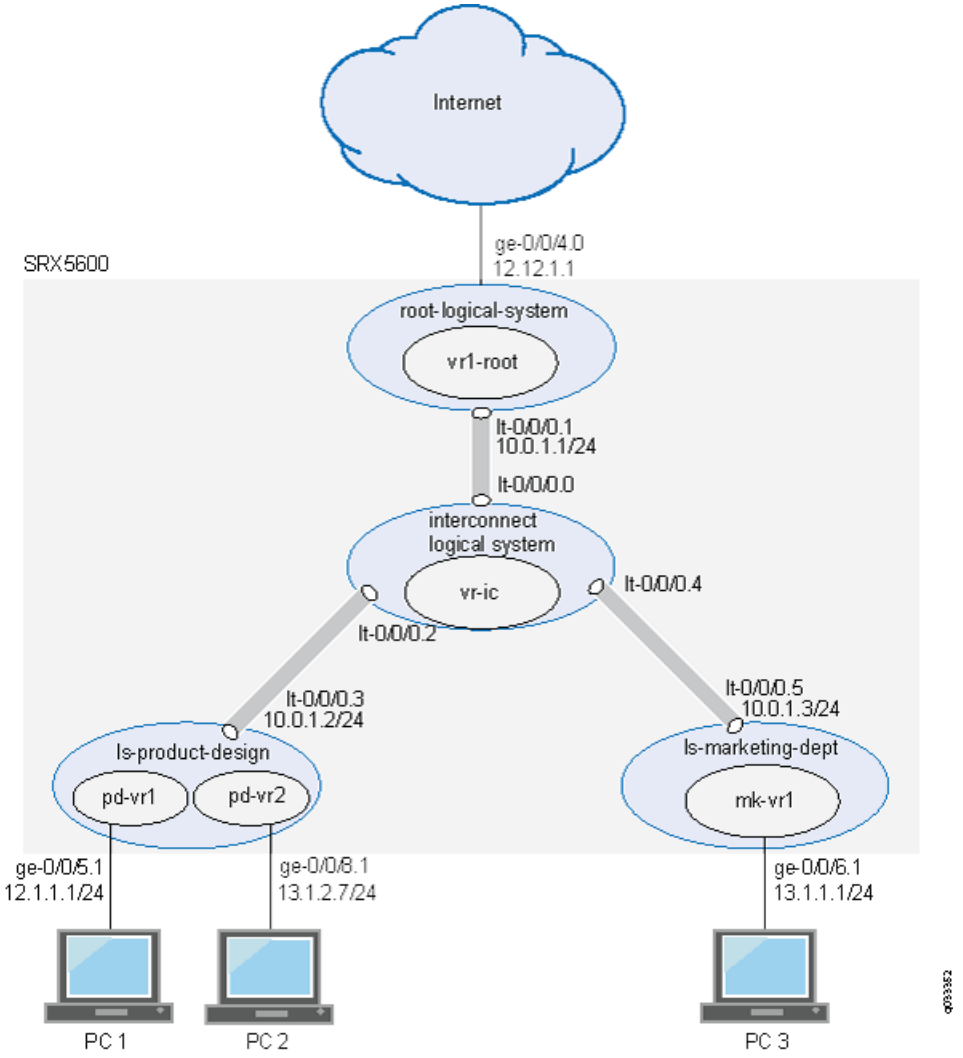
Understanding Flow in Logical Systems for SRX Series Devices

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 inforrmation 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 12.

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



- Understanding Junos OS SRX Series Services Gateways Architecture on page 13
- Session Creation for Devices Running Logical Systems on page 14
- Understanding Flow on Logical Systems on page 14
- Understanding Packet Classification on page 14
- Handling Pass-Through Traffic for Logical Systems on page 15
- Handling Self-Traffic on page 16
- Understanding Session and Gate Limitation Control on page 18

- Understanding Sessions on page 18
- About Configuring Sessions on page 18

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 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.

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 12.

- 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).

Consider how pass-through traffic is handled across logical systems in the topology shown in Figure 2 on page 12.

- 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 12.

- 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 12.

- 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.

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

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

- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 10
- Understanding Logical Systems for SRX Series Services Gateways on page 3

PART 2

Part 2 Configuration

This part explains how to configure an SRX Series device for logical systems. It includes example configurations that a master administrator would create to manage the master logical system and the device, including creating user logical systems, and example configurations that users logical system administrators would create for their logical system.

CHAPTER 2

Master Logical System Configuration

SRX Series Logical System Master Administrator Configuration Tasks Overview

This topic identities and describes the master administrator's tasks in the order in which they are performed.

An SRX Series device running logical systems is managed by a master administrator. The master administrator has the same capabilities as the root administrator of an SRX Series device not running logical systems. However, the master administrator's role and responsibilities extend beyond those of other SRX Series device administrators because an SRX Series device running logical systems is partitioned into discrete logical systems, each with its own resources, configuration, and management concerns. The master administrator is responsible for creating these user logical systems and provisioning them with resources.

For an overview of the master administrator's role and responsibilities, see "Understanding the Master Logical System and the Master Administrator Role" on page 8.

As the master administrator, you perform the following tasks to configure an SRX Series device running logical systems:

1. Configure a root password. Initially the master administrator logs in to the device as the root user without needing to specify a password. After you log in to the device, you must define a root password for later use.

   See "Example: Configuring a Root Password for the Device" on page 26 for configuration information.

2. Create user logical systems and their administrators and users. Optionally, create an interconnect logical system.

   For each user logical system that you want to configure on the device, you must create a logical system, define one or more administrators for it, and add users to it.

   The master administrator configures login accounts for user logical system administrators and users and associates them with the user logical system. A user logical system can have more than one administrator; the master administrator must define and add all user logical system administrators and add them to their user logical systems.

   The master administrator adds users to user logical systems on behalf of the user logical system administrator. For example, if you have created a user logical system for the product design department, you must create user accounts for the users who belong to that department and associate them with the user logical system. The user logical system administrator does not have the ability to do this. Rather, the user logical administrator tells you the user accounts that you must create and add for his logical system.

   If you intend to use an internal virtual private LAN service (VPLS) switch to allow logical systems to communicate with one another, you must create an interconnect logical system. An interconnect logical system does not require an administrator.

   - For configuration information, see "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26
   - For information on user logical system administrators, see "Understanding User Logical Systems and the User Logical System Administrator Role" on page 9.
   - For information on the interconnect logical system, see "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 10.

3. Configure one or more security profiles. Security profiles assign security resources to logical systems. You can assign a single security profile to more than one logical system if you intend to allocate the same kinds and amounts of resources to them.

   - For configuration information, see "Example: Configuring Logical Systems Security Profiles" on page 40.
   - For information on security profiles, see "Understanding Logical Systems Security Profiles" on page 34.

4. Configure interfaces, routing instances, and static routes for logical systems, as appropriate.
   - If you plan to use an interconnect logical system, configure its logical tunnel interfaces and add them to its virtual routing instance.
   - Configure interfaces for the master logical system. Optionally, create its logical tunnel interface to allow it to communicate with other logical systems on the device. Create a virtual routing instance for the master logical system and add its interfaces and static routes to it. Also configure logical interfaces for user logical systems with VLAN tagging.

     NOTE: **The master administrator tells the user logical system administrators which interfaces are assigned to their logical systems. It is the user logical system administrator's responsibility to configure their interfaces.**

   - Optionally, configure logical tunnel interfaces for any user logical systems that you want to allow to communicate with one another using the internal VPLS switch.
   - For configuration information, see "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for User Logical Systems" on page 47.
   - For information about the interconnect logical system and logical tunnel (lt-0/0/0) interfaces, see "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 10.
5. Enable CPU utilization control and configure the CPU control target and reserved CPU quotas for logical systems. See "Example: Configuring CPU Utilization" on page 59.
6. Optionally, configure dynamic routing protocols for the master logical system. See "Example: Configuring OSPF Routing Protocol for the Master Logical System" on page 62
7. Configure zones, security policies, and security features for the master logical system. See "Example: Configuring Security Features for the Master Logical System" on page 66.
8. Configure IDP for the master logical system. See "Example: Configuring an IDP Policy for the Master Logical System" on page 71.
9. Configure application firewall services on the master logical system. See "Understanding Logical System Application Firewall Services" on page 137 and "Example: Configuring Application Firewall Services for a Master Logical System" on page 77.
10. Configure a route-based VPN to secure traffic between a logical system and a remote site. See "Example: Configuring IKE and IPsec SAs for a VPN Tunnel" on page 116.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems for SRX Series Services Gateways on page 3

Example: Configuring a Root Password for the Device

Requirements

Before you begin, read "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 to understand how this task fits into the overall configuration process.

The example uses an SRX5600 device running Junos OS with logical systems.

Overview

The Junos OS software is installed on the router before it is delivered from the factory. When you power on your router, it is ready for you to configure. Initially you log in as *root* user without using a password.

After you log in, you can configure a password for the root user, or, in logical systems terms, the master administrator. The master administrator has root privileges over the device.

Configuration

Configuring the Root Password

Step-by-Step Procedure

1. Configure a root password for the device.

   ```
   user@host# set system root-authentication Talk22rt6
   ```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding Logical Systems for SRX Series Services Gateways on page 3

Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System

This example shows how to create user logical systems and assign administrators to them. It shows how to add users to a user logical system. And the example shows how to create an interconnect logical system, which is optional.

NOTE: Only the master administrator can create user login accounts for administrators and users. If a user logical system administrator wants to add users to his logical system, he must convey the information to the master administrator, who will add the users.

Requirements

The example uses an SRX5600 device running Junos OS with logical systems.

Overview

Before you begin, read "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 to understand how this task fits into the overall configuration process.

This example is for a company that includes product design, marketing, and accounting departments. The company wants to curtail hardware and energy costs, but not at the risk of exposing data across departments or to the Internet.

Each department has its own security requirements in regard both to other departments and to the Internet. To meet its requirements for cost control without forfeiting security, the company deploys the SRX5600 device. The master administrator configures three user logical systems giving each department a logical device that is private and fully secured.

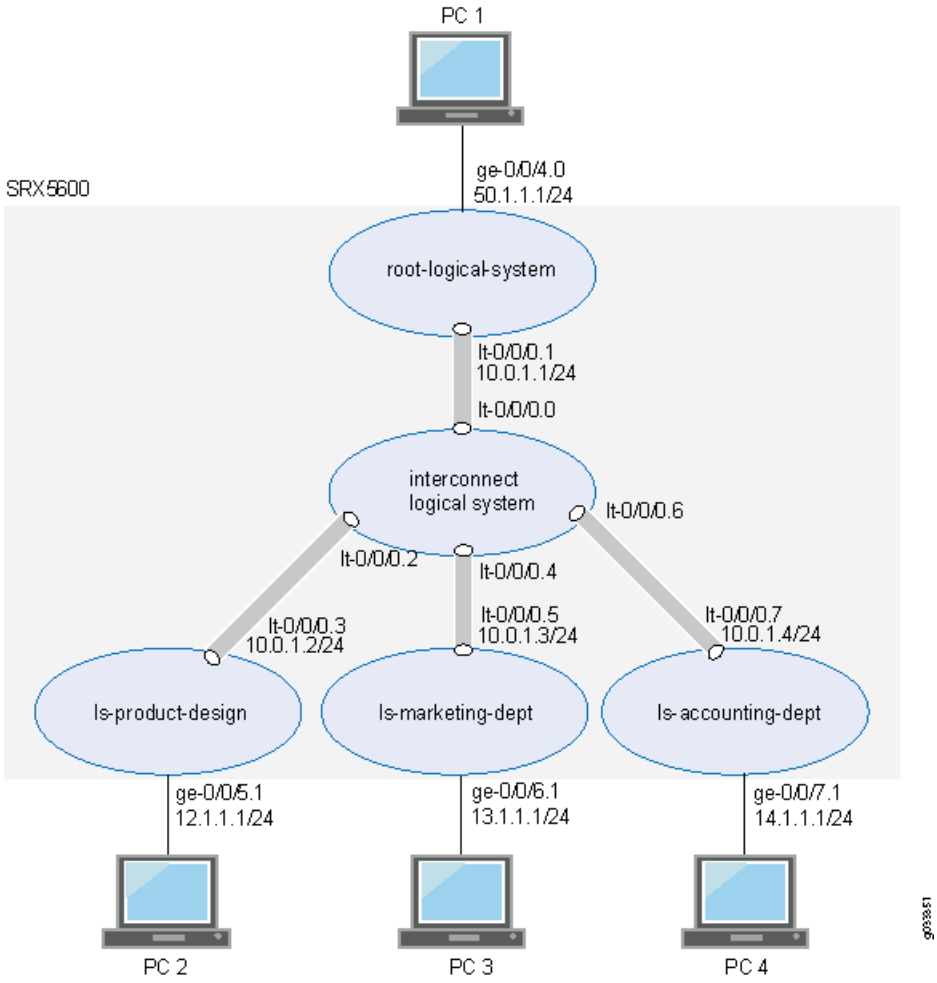
This topic covers how to:

- Create user logical systems and an interconnect logical system that is used as an internal VPLS switch to allow traffic to pass from one logical system to another.
- Create administrators for user logical systems other than the interconnect logical system. A user logical system can have more than one administrator. The interconnect logical system does not require an administrator.
- Add users to a user logical system.

NOTE: This example shows how to configure only two users—lsdesignuser1 and lsdesignuser2. In reality, every user logical system will include many users that would require configurations similar to those shown in this example.

Figure 3 on page 28 shows an SRX5600 device deployed and configured for logical systems. The configuration examples reflect this deployment.

Figure 3: SRX Series Device Configured for Logical Systems



Configuration

Configuring User Logical Systems, Their Administrators, Their Users, and an Interconnect 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 logical-systems ls-product-design
set system login class ls-design-admin logical-system ls-product-design
set system login class ls-design-admin permissions all
set system login user lsdesignadmin1 full-name lsdesignadmin1
set system login user lsdesignadmin1 class ls-design-admin
```

```
set system login user lsdesignadmin1 authentication encrypted-password
  "$1$VYfdRheI$CMSegr7Zi9RG4JNKa90iS/"
set system login class ls-design-user logical-system ls-product-design
set system login class ls-design-user permissions view
set system login user lsdesignuser1 full-name lsdesignuser1
set system login user lsdesignuser1 class ls-design-user
set system login user lsdesignuser1 authentication encrypted-password
  "$1$7tUK.xiD$NrODFcA1r5mRAFfP2ltXt0"
set system login user lsdesignuser2 full-name lsdesignuser2
set system login user lsdesignuser2 class ls-design-user
set system login user lsdesignuser2 authentication encrypted-password
  "$1$KLh7M1ri$QhWyFK76lNfIJ0cJv0Wic0"
set logical-systems ls-marketing-dept
set system login class ls-marketing-admin logical-system ls-marketing-dept
set system login class ls-marketing-admin permissions all
set system login user lsmarketingadmin1 class ls-marketing-admin
set system login user lsmarketingadmin1 full-name lsmarketingadmin1
set system login user lsmarketingadmin1 authentication encrypted-password
  "$1$vEJdnI3F$/srH5kEqO/bUhsbOOWxXB."
set system login user lsmarketingadmin2 full-name lsmarketingadmin2
set system login user lsmarketingadmin2 class ls-marketing-admin
set system login user lsmarketingadmin2 authentication encrypted-password
  "$1$ANlhADCm$UKnXtRMajiDxhREL2XA5k."
set logical-systems ls-accounting-dept
set system login class ls-accounting-admin logical-system ls-accounting-dept
set system login class ls-accounting-admin permissions all
set system login user lsaccountingadmin1 full-name lsaccountingadmin1
set system login user lsaccountingadmin1 class ls-accounting-admin
set system login user lsaccountingadmin1 authentication encrypted-password
  "$1$qZt6lVFr$NfjsX9pe7CsKzveNnIUz11"
set logical-systems interconnect-logical-system
```

Step-by-Step Procedure

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

1. Create the first user logical system and define its administrator.

   a. Create the user logical system.

      ```
      [edit]
      user@host# set logical-systems ls-product-design
      ```

   b. Assign the user login class to the user logical system.

      ```
      [edit system]
      user@host# set login class ls-design-admin logical-system ls-product-design
      ```

   c. Create the login class to give the user logical system administrator full permission over the user logical system.

      ```
      [edit system]
      user@host# set login class ls-design-admin permissions all
      ```

   d. Assign a full name to the user logical system administrator.

      ```
      [edit system]
      ```

```
user@host# set login user lsdesignadmin1 full-name lsdesignadmin1
```

e. Associate the login class with the user logical system administrator to allow the administrator to log in to the user logical system.

```
[edit system]
user@host# set login user lsdesignadmin1 class ls-design-admin
```

f. Create a user login password for the user logical system administrator.

```
[edit system]
user@host# set login user lsdesignadmin1 authentication plain-text-password
New password: Talk1234
Retype new password: Talk1234
```

2. Configure the first user for the logical system.

a. Configure the user login class and assign it to the user logical system.

```
[edit system]
user@host# set login class ls-design-user logical-system ls-product-design
```

b. To give the first user the ability to see the logical system's resources and settings but not change them, assign **view** as the permission to the login class.

```
[edit system]
user@host# set login class ls-design-user permissions view
```

c. Assign a full name to the logical system user.

```
[edit system]
user@host# set login user lsdesignuser1 full-name lsdesignuser1
```

d. Associate the login class with the user to allow the user to log in to the user logical system.

```
user@host# set login user lsdesignuser1 class ls-design-user
```

e. Create a user login password for the user.

```
[edit system]
user@host# set login user lsdesignuser1 authentication plain-text-password
New password: Talk4234
Retype new password: Talk4234
```

3. Create the second user for logical system ls-product-design.

a. Assign a full name to the user.

```
[edit system]
user@host# set login user lsdesignuser2 full-name lsdesignuser2
```

b. Associate the user with the login class to allow the user to log in to the user logical system.

```
user@host# set login user lsdesignuser2 class ls-design-user
```

c. Create a user login password.

```
[edit system]
user@host# set login user lsdesignuser2 authentication plain-text-password
```



```
New password: Talk9234
Retype new password: Talk9234
```

4. Create the second user logical system and define its administrator.

   a. Create the user logical system.

   ```
   [edit]
   user@host# set logical-systems ls-marketing-dept
   ```

   b. Configure the user login class and assign it to the user logical system.

   ```
   [edit system]
   user@host# set login class ls-marketing-admin logical-system ls-marketing-dept
   ```

   c. To give the user logical system administrator control over the user logical system, assign **all** as the permissions to the login class.

   ```
   [edit system]
   user@host# set login class ls-marketing-admin permissions all
   ```

   d. Assign a full name to the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsmarketingadmin1 full-name lsmarketingadmin1
   ```

   e. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

   ```
   [edit system]
   user@host# set login user lsmarketingadmin1 class ls-marketing-admin
   ```

   f. Create a user login password for the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsmarketingadmin1 authentication plain-text-password
   New password: Talk2345
   Retype new password: Talk2345
   ```

5. Create a second user logical system administrator for the ls-marketing-dept logical system.

   a. Assign a full name to the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsmarketingadmin2 full-name lsmarketingadmin2
   ```

   b. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

   ```
   [edit system]
   user@host# set login lsmarketingadmin2 class ls-marketing-admin
   ```

   c. Create a user login password for the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsmarketingadmin2 authentication plain-text-password
   New password: Talk6345
   ```

```
Retype new password: Talk6345
```

6. Create the third user logical system and define its administrator.

   a. Create the user logical system.

   ```
   [edit]
   user@host# set logical-systems ls-accounting-dept
   ```

   b. Configure the user login class and assign it to the user logical system.

   ```
   [edit system]
   user@host# set login class ls-accounting-admin logical-system
     ls-accounting-dept
   ```

   c. To give the user logical system administrator control over the user logical system, assign permissions to the login class.

   ```
   [edit system]
   user@host# set login class ls-accounting-admin permissions all
   ```

   d. Assign a full name to the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsaccountingadmin1 full-name lsaccountingadmin1
   ```

   e. Associate the user logical system administrator with the login class to allow the administrator to log in to the user logical system.

   ```
   [edit system]
   user@host# set login user lsaccountingadmin1 class ls-accounting-admin
   ```

   f. Create a login password for the user logical system administrator.

   ```
   [edit system]
   user@host# set login user lsaccountingadmin1 authentication
     plain-text-password
   New password: Talk5678
   Retype new password: Talk5678
   ```

7. Configure an interconnect logical system to allow logical systems to pass traffic from one to another.

   ```
   user@host# set logical-systems interconnect-logical-system
   ```

Results From configuration mode, confirm your configuration by entering the **show logical-systems** command to verify that the logical systems were created. Also enter the **show system login class** command for each class that you defined.

To ensure that the logical systems administrators were created, enter the **show system login user** command.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems ?
interconnect-logical-system;
ls-accounting-dept;
```



```
ls-marketing-dept;
ls-product-design;

user@host# show system login class ls-design-admin
logical-system ls-product-design;
permissions all;

user@host# show system login class ls-design-user
logical-system ls-product-design
permissions view;

user@host show system login class ls-marketing-admin
logical-system ls-marketing-dept;
permissions all;

user@host show system login class ls-accounting-admin
logical-system ls-accounting-dept;
permissions all;

user@host show system login user ?
lsaccountingadmin1 lsaccountingadmin1
lsdesignadmin1 lsdesignadmin1
lsdesignuser2 lsdesignuser2
lsmarketingadmin1 lsmarketingadmin1
lsmarketingadmin2 lsmarketingadmin2
```

Verification

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

- Verifying User Logical Systems and Login Configurations from the Master Logical System on page 33
- Verifying User Logical Systems and Login Configurations Using Telnet on page 34

Verifying User Logical Systems and Login Configurations from the Master Logical System

Purpose Verify that the user logical systems exist and that you, as the master administrator, can enter them from root. Return from a user logical system to the master logical system.

Action From operational mode, enter the following command:

```
root@host> set cli logical-system ls-product-design
Logical system:ls-product-design
root@host:ls-product-design>

root@host:ls-product-design> clear cli logical-system
Cleared default logical system
root@host>

root@host> set cli logical-system ls-marketing-dept
Logical system:ls-marketing-dept
root@host:ls-marketing-dept>

root@host:ls-marketing-dept> clear cli logical-system
Cleared default logical system
root@host>
```

```
root@host> set cli logical-system ls-accounting-dept
Logical system:ls-accounting-dept
root@host:ls-accounting-dept>

root@host:ls-accounting-dept> clear cli logical-system
Cleared default logical system
root@host>
```

Verifying User Logical Systems and Login Configurations Using Telnet

Purpose Verify that the user logical systems you created exist and that the administrators' login IDs and passwords that you created are correct.

Action Use Telnet to log in to each user logical system as its user administrator would do.

1. Run Telnet specifying the IP address of your SRX Series device. For example:

   ```
   telnet 10.11.11.19
   ```

2. Enter the login ID and password for the administrator for one of the user logical systems that you created. After you log in, the prompt shows the administrator name. Notice how this result differs from the result produced when you log in to the user logical system from the master logical system at root. Repeat this procedure for all of your user logical systems.

   ```
   login: lsdesignadmin1
   Password: Talk1234
   lsdesignadmin1@host: ls-product-design>
   ```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Logical Systems Security Profiles on page 40
- Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for User Logical Systems on page 47

Understanding Logical System Security Profiles

Logical systems allow you to virtually divide a supported SRX Series device into multiple devices, isolating one from another, securing them from intrusion and attacks, and protecting them from faulty conditions outside their own contexts. To protect logical systems, security resources are configured in a manner similar to how they are configured for a discrete device. However, as the master administrator, you must allocate the kinds and amounts of security resources to logical systems. The logical system administrator allocates resources for his own logical system.

An SRX Series device running logical systems can be partitioned into user logical systems, an interconnect logical system, if desired, and the default master logical system. When the system is initialized, the master logical system is created at the root level. All system resources are assigned to it, effectively creating a default master logical system security profile. To distribute security resources across logical systems, the master administrator

creates security profiles that specify the kinds and amounts of resources to be allocated to a logical system that the security profile is bound to. Only the master administrator can configure security profiles and bind them to logical systems. The user logical system administrator configures these resources for his logical system.

Logical systems are defined largely by the resources allocated to them, including security components, interfaces, routing instances, static routes, and dynamic routing protocols. When the master administrator configures a user logical system, he binds a security profile to it. Any attempt to commit a configuration for a user logical system without a security profile bound to it will fail.

This topic includes the following sections:

Logical Systems Security Profiles

As master administrator, you can configure a single security profile to assign resources to a specific logical system, use the same security profile for more than one logical system, or use a mix of both methods. You can configure up to 32 security profiles on an SRX Series device running logical systems. When you reach the limit, you must delete a security profile and commit the configuration change before you can create and commit another security profile. In many cases fewer security profiles are needed because you might bind a single security profile to more than one logical system.

Security profiles allow you to:

- Share the device's resources, including policies, zones, addresses and address books, flow sessions, and various forms of NAT, among all logical systems appropriately. You can dedicate various amounts of a resource to the logical systems and allow them to compete for use of the free resources.

  Security profiles protect against one logical system exhausting a resource that is required at the same time by other logical systems. Security profiles protect critical system resources and maintain a fair level of performance among user logical systems when the device is experiencing heavy traffic flow. They defend against one user logical system dominating the use of resources and depriving other user logical systems of them.

- Configure the device in a scalable way to allow for future creation of additional user logical systems.

You must delete a logical system's security profile before you delete that logical system.

How the System Assesses Resources Assignment and Use Across Logical Systems

To provision a logical system with security resources, you, as a master administrator, configure a security profile that specifies for each resource:

- A reserved quota that guarantees that the specified resource amount is always available to the logical system.
- A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems must compete for global resources.

If a reserved quota is not configured for a resource, the default value is 0. If a maximum allowed quota is not configured for a resource, the default value is the global system quota for the resource (global system quotas are platform-dependent). The master administrator must configure appropriate maximum allowed quota values in the security profiles so the maximum resource usage of a specific logical system does not negatively impact other logical systems configured on the device. The master administrator must configure the appropriate maximum-allowed quota values in the security profiles so that the maximum resource usage of a specific logical system does not negatively impact other logical systems configured on the device.

The system maintains a count of all allocated resources that are reserved, used, and made available again when a logical system is deleted. This count determines whether resources are available to use for new logical systems or to increase the amount of the resources allocated to existing logical systems through their security profiles.

When a user logical system is deleted, its reserved resource allocations are released for use by other logical systems.

Resources configured in security profiles are characterized as static modular resources or dynamic resources. For static resources, we recommend setting a maximum quota for a resource equal or close to the amount specified as its reserved quota, to allow for scalable configuration of logical systems. A high maximum quota for a resource might give a logical system greater flexibility through access to a larger amount of that resource, but it would constrain the amount available to allocate to a new user logical system.

The difference between reserved and maximum allowed amounts for a dynamic resource is not important because dynamic resources are aged out and do not deplete the pool available for assignment to other logical systems.

The following resources can be specified in a security profile:

- Security policies, including schedulers
- Security zones
- Addresses and address books for security policies

- Application firewall rule sets
- Application firewall rules
- Firewall authentication
- Flow sessions and gates
- NAT, including:
  - Cone NAT bindings
  - NAT destination rule
  - NAT destination pool
  - NAT IP address in source pool without port address translation (PAT)
  - NAT IP address in source pool with PAT
  - NAT port overloading
  - NAT source pool
  - NAT source rule
  - NAT static rule

NOTE:

All resources except flow sessions are static.

You can modify a logical system security profile dynamically while the security profile is assigned to other logical systems. However, to ensure that the system resource quota is not exceeded, the system takes the following actions:

- If a static quota is changed, system daemons that maintain logical system counts for resources specified in security profiles revalidate the security profile. This check identifies the number of resources assigned across all logical systems to determine whether the allocated resources, including their increased amounts, are available.

  These quota checks are the same quota checks that the system performs when you add a new user logical system and bind a security profile to it. The are also performed when you bind a different security profile from the security profile that is presently assigned to it to an existing user logical system (or the master logical system).
- If a dynamic quota is changed, no check is performed, but the new quota is imposed on future resource usage.

Cases: Assessments of Reserved Resources Assigned through Security Profiles

To understand how the system assesses allocation of reserved resources through security profiles, consider the following three cases that address allocation of one resource, zones. To keep the example simple, 10 zones are allocated in security-profile-1: 4 reserved zones

and 6 maximum zones. This example assumes that the full maximum amount specified—six zones—is available for the user logical systems. The system maximum number of zones is 10.

These cases address configuration across logical systems. They test to see whether a configuration will succeed or fail when it is committed based on allocation of zones.

Table 3 on page 38 shows the security profiles and their zone allocations.

Table 3: Security Profiles Used for Reserved Resource Assessments

Two Security Profiles Used in the Configuration Cases
security-profile-1 • zones reserved quota = 4 • zones maximum quota = 6 NOTE: Later the master administrator dynamically increases the reserved zone count specified in this profile.
master-logical-system-profile • zones maximum quota = 10 • no reserved quota

Table 4 on page 39 shows three cases that illustrate how the system assesses reserved resources for zones across logical systems based on security profile configurations.

- The configuration for the first case succeeds because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 8, which is less than the system maximum resource quota.
- The configuration for the second case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 12, which is greater than the system maximum resource quota.
- The configuration for the third case fails because the cumulative reserved resource quota for zones configured in the security profiles bound to all logical systems is 12, which is greater than the system maximum resource quota.

Table 4: Reserved Resource Allocation Assessment Across Logical Systems

Reserved Resource Quota Checks Across Logical Systems
Example 1: Succeeds This configuration is within bounds: 4+4+0=8, maximum capacity =10. Security Profiles Used • The security profile security-profile-1 is bound to two user logical systems: user-logical-system-1 and user-logical-system-2. • The master-logical-system-profile profile is used exclusively for the master logical system. • user-logical-system-1 = 4 reserved zones. • user-logical-system-2 = 4 reserved zones. • master-logical-system = 0 reserved zones.
Example 2: Fails This configuration is out of bounds: 4+4+4=12, maximum capacity =10. • user-logical-system-1 = 4 reserved zones. • user-logical-system-2 = 4 reserved zones. • master-logical-system = 0 reserved zones. • new-user-logical-system = 4 reserved zones. Security Profiles • The security profile security-profile-1 is bound to two user logical systems: user-logical-system-1 and user-logical-system-2. • The master-logical-system-profile is bound to the master logical system and used exclusively for it. • The master administrator configures a new user logical system called new-user-logical-system and binds security-profile-1 to it.
Example 3: Fails This configuration is out of bounds: 6+6=12, maximum capacity =10. The master administrator modifies the reserved zones quota in security-profile-1, increasing the count to 6. • user-logical-system-1 = 6 reserved zones. • user-logical-system-2 = 6 reserved zones. • master-logical-system = 0 reserved zones.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Logical Systems Security Profiles on page 40
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Example: Configuring Logical Systems Security Profiles

This example shows how a master administrator configures three logical system security profiles to assign to user logical systems and the master logical system to provision them with security resources.

Requirements

The example uses an SRX5600 device running Junos OS with logical systems.

Before you begin, read "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 to understand how this task fits into the overall configuration process.

Overview

This example shows how to configure security profiles for the following logical systems:

- The root-logical-system logical system. The security profile master-profile is assigned to the master, or root, logical system.
- The ls-product-design logical system. The security profile ls-design-profile is assigned to the logical system.
- The ls-marketing-dept logical system. The security profile ls-accnt-mrkt-profile is assigned to the logical system.
- The ls-accounting-dept logical system. The security profile ls-accnt-mrkt-profile is assigned to the logical system.
- The interconnect-logical-system, if you use one. You must assign a dummy, or null, security profile to it.

This configuration relies on the deployment shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26.

Configuration

Configuring Logical System Security Profiles

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 system security-profile master-profile policy maximum 65
set system security-profile master-profile policy reserved 60
set system security-profile master-profile zone maximum 22
set system security-profile master-profile zone reserved 17
set system security-profile master-profile flow-session maximum 3000
set system security-profile master-profile flow-session reserved 2100
set system security-profile master-profile nat-nopat-address maximum 115
set system security-profile master-profile nat-nopat-address reserved 100
set system security-profile master-profile nat-static-rule maximum 125
set system security-profile master-profile nat-static-rule reserved 100
set system security-profile master-profile idp
set system security-profile master-profile logical-system root-logical-system
set system security-profile ls-accnt-mrkt-profile policy maximum 65
set system security-profile ls-accnt-mrkt-profile policy reserved 60
set system security-profile ls-accnt-mrkt-profile zone maximum 22
set system security-profile ls-accnt-mrkt-profile zone reserved 17
set system security-profile ls-accnt-mrkt-profile flow-session maximum 2500
set system security-profile ls-accnt-mrkt-profile flow-session reserved 2000
set system security-profile ls-accnt-mrkt-profile nat-nopat-address maximum 125
set system security-profile ls-accnt-mrkt-profile nat-nopat-address reserved 100
set system security-profile ls-accnt-mrkt-profile nat-static-rule maximum 125
set system security-profile ls-accnt-mrkt-profile nat-static-rule reserved 100
set system security-profile ls-accnt-mrkt-profile logical-system ls-marketing-dept
set system security-profile ls-accnt-mrkt-profile logical-system ls-accounting-dept
set system security-profile ls-design-profile policy maximum 50
set system security-profile ls-design-profile policy reserved 40
set system security-profile ls-design-profile zone maximum 10
set system security-profile ls-design-profile zone reserved 5
set system security-profile ls-design-profile flow-session maximum 2500
set system security-profile ls-design-profile flow-session reserved 2000
set system security-profile ls-design-profile nat-nopat-address maximum 120
set system security-profile ls-design-profile nat-nopat-address reserved 100
set system security-profile ls-design-profile logical-system ls-product-design
set system security-profile interconnect-profile logical-system
  interconnect-logical-system
```

Step-by-Step Procedure

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

Create three security profiles.

1. Create the first security profile.

   a. Specify the number of maximum and reserved policies.

      ```
      [edit system security-profile]
      user@host# set master-profile policy maximum 65 reserved 60
      ```

   b. Specify the number of maximum and reserved zones.

      ```
      [edit system security-profile]
      user@host# set master-profile zone maximum 22 reserved 17
      ```

   c. Specify the number of maximum and reserved sessions.

      ```
      [edit system security-profile]
      ```

```
user@host# set master-profile flow-session maximum 3000 reserved 2100
```

d. Specify the number of maximum and reserved source NAT no-PAT addresses and static NAT rules.

```
[edit system security-profile]
user@host# set master-profile nat-nopat-address maximum 115 reserved 100
user@host# set master-profile nat-static-rule maximum 125 reserved 100
```

e. Enable intrusion detection and prevention (IIDP). You can enable IDP only for the master (root) logical system.

```
[edit system security-profile]
user@host# set idp
```

f. Bind the security profile to the logical system.

```
[edit system security-profile]
user@host# set master-profile logical-system root-logical-system
```

2. Create the second security profile.

a. Specify the number of maximum and reserved policies.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile policy maximum 65 reserved 60
```

b. Specify the number of maximum and reserved zones.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile zone maximum 22 reserved 17
```

c. Specify the number of maximum and reserved sessions.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile flow-session maximum 2500 reserved
  2000
```

d. Specify the number of maximum and reserved source NAT no-PAT addresses.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile nat-nopat-address maximum 125 reserved
  100
```

e. Specify the number of maximum and reserved static NAT rules.

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile nat-static-rule maximum 125 reserved 100
```

f. Bind the security profile to two logical systems.

```
[edit system]
user@host# set security-profile ls-accnt-mrkt-profile logical-system
  ls-marketing-dept
user@host# set security-profile ls-accnt-mrkt-profile logical-system
  ls-accounting-dept
```

3. Create the third security profile.

a. Specify the number of maximum and reserved policies.

```
[edit system security-profile]
user@host# set ls-design-profile policy maximum 50 reserved 40
```

b. Specify the number of maximum and reserved zones.

```
[edit system security-profile]
user@host# set ls-design-profile zone maximum 10 reserved 5
```

c. Specify the number of maximum and reserved sessions.

```
[edit system security-profile]
user@host# set ls-design-profile flow-session maximum 2500 reserved 2000
```

d. Specify the number of maximum and reserved source NAT no-PAT addresses.

```
[edit system security-profile]
user@host# set ls-design-profile nat-nopat-address maximum 120 reserved 100
```

4. Bind the security profile to a logical system.

```
user@host# set system security-profile ls-design-profile logical-system
  ls-product-design
```

5. Bind a null security profile to the interconnect logical system.

```
user@host# set system security-profile interconnect-profile logical-system
  interconnect-logical-system
```

Results From configuration mode, confirm your configuration by entering the **show system security-profile** command to see all security profiles configured.

To see individual security profiles, enter the **show system security-profile master-profile**, the **show system security-profile ls-accnt-mrkt-profile** and, the **show system security-profile ls-design-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show system security-profile
  interconnect-profile {
    logical-system interconnect-logical-system;
  }
    ls-accnt-mrkt-profile {
      policy {
        maximum 65;
        reserved 60;
      }
      zone {
        maximum 22;
        reserved 17;
      }
      flow-session {
        maximum 2500;
        reserved 2000;
      }
      nat-nopat-address {
        maximum 125;
        reserved 100;
      }
```

```
    nat-static-rule {
      maximum 125;
      reserved 100;
    }
    logical-system [ ls-marketing-dept ls-accounting-dept ];
  }
  ls-design-profile {
    policy {
      maximum 50;
      reserved 40;
    }
    zone {
      maximum 10;
      reserved 5;
    }
    flow-session {
      maximum 2500;
      reserved 2000;
    }
    nat-nopat-address {
      maximum 120;
      reserved 100;
    }
    nat-static-rule {
      maximum 125;
      reserved 100;
    }
    logical-system ls-product-design;
  }
  master-profile {
    policy {
      maximum 65;
      reserved 60;
    }
    zone {
      maximum 22;
      reserved 17;
    }
    flow-session {
      maximum 3000;
      reserved 2100;
    }
    nat-nopat-address {
      maximum 115;
      reserved 100;
    }
    nat-static-rule {
      maximum 125;
      reserved 100;
    }
    root-logical-system;
  }
```

```
user@host# show system security-profile master-profile
    policy {
      maximum 65;
```

```
        reserved 60;
        }
        zone {
          maximum 22;
          reserved 17;
        }
        flow-session {
          maximum 3000;
          reserved 2100;
        }
        nat-nopat-address {
          maximum 115;
          reserved 100;
        }
        nat-static-rule {
          maximum 125;
          reserved 100;
        }
      root-logical-system;
```

```
user@host# show system security-profile ls-accnt-mrkt-profile
  policy {
    maximum 65;
    reserved 60;
    }
    zone {
      maximum 22;
      reserved 17;
    }
    flow-session {
      maximum 2500;
      reserved 2000;
    }
    nat-nopat-address {
      maximum 125;
      reserved 100;
    }
    nat-static-rule {
      maximum 125;
      reserved 100;
    }
  logical-system [ ls-accounting-dept ls-marketing-dept ];
```

```
user@host# show system security-profile ls-design-profile
  policy {
    maximum 50;
    reserved 40;
    }
    zone {
      maximum 10;
      reserved 5;
    }
    flow-session {
      maximum 2500;
      reserved 2000;
    }
    nat-nopat-address {
```

```
    maximum 120;
    reserved 100;
  }
  nat-static-rule {
    maximum 125;
    reserved 100;
  }
logical-system ls-product-design;
```

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

Verification

To confirm that the security resources that you allocated for logical systems have been assigned to them, follow this procedure for each logical system and for all its resources.

- Verifying That Security Profile Resources Are Effectively Allocated for Logical Systems on page 46

Verifying That Security Profile Resources Are Effectively Allocated for Logical Systems

Purpose Verify security resources for each logical system. Follow this process for all configured logical systems.

Action

1. Use Telnet to log into each user logical system as its user logical system administrator.

   Run Telnet, specifying the IP address of your SRX Series device. For example:

   ```
   telnet 10.11.11.19
   ```

2. Enter the login ID and password for one of the user logical systems that you created

   ```
   login: lsmarketingadmin1
   password: Talk2345
   lsmarketingadmin1@host:ls-marketing-dept>
   ```

3. Enter the following statement to Identify the resources configured for the profile.

   ```
   lsmarketingadmin1@host:ls-marketing-dept> show system security-profile ?
   ```

4. Enter the following command at the resulting prompt. Do this for each feature configured for the profile.

   ```
   lsmarketingadmin1@host:ls-marketing-dept> show system security-profile zone detail
   logical system name : ls-marketing-dept
   security profile name : ls-accnt-mrkt-profile
   used amount : 0
   reserved amount : 17
   maximum quota : 22
   ```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems Security Profiles on page 34
- Understanding the Master Logical System and the Master Administrator Role on page 8

- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems

This topic covers configuration of interfaces, static routes, and routing instances for the master and interconnect logical systems. It also covers configuration of logical tunnel interfaces for user logical systems.

Requirements

The example uses an SRX5600 device running Junos operating system (Junos OS) with logical systems.

Before you begin:

- Read "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 to understand how and where this procedure fits in the overall master administrator configuration process.
- Read "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 10

Overview

This scenario shows how to configure interfaces for the logical systems on the device, including an interconnect logical system.

- For the interconnect logical system, the example configures logical tunnel interfaces lt-0/0/0.0, lt-0/0/0.2, lt-0/0/0.4, and lt-0/0/0.6. The example configures a routing instance called vr-ic and assigns the interfaces to it.

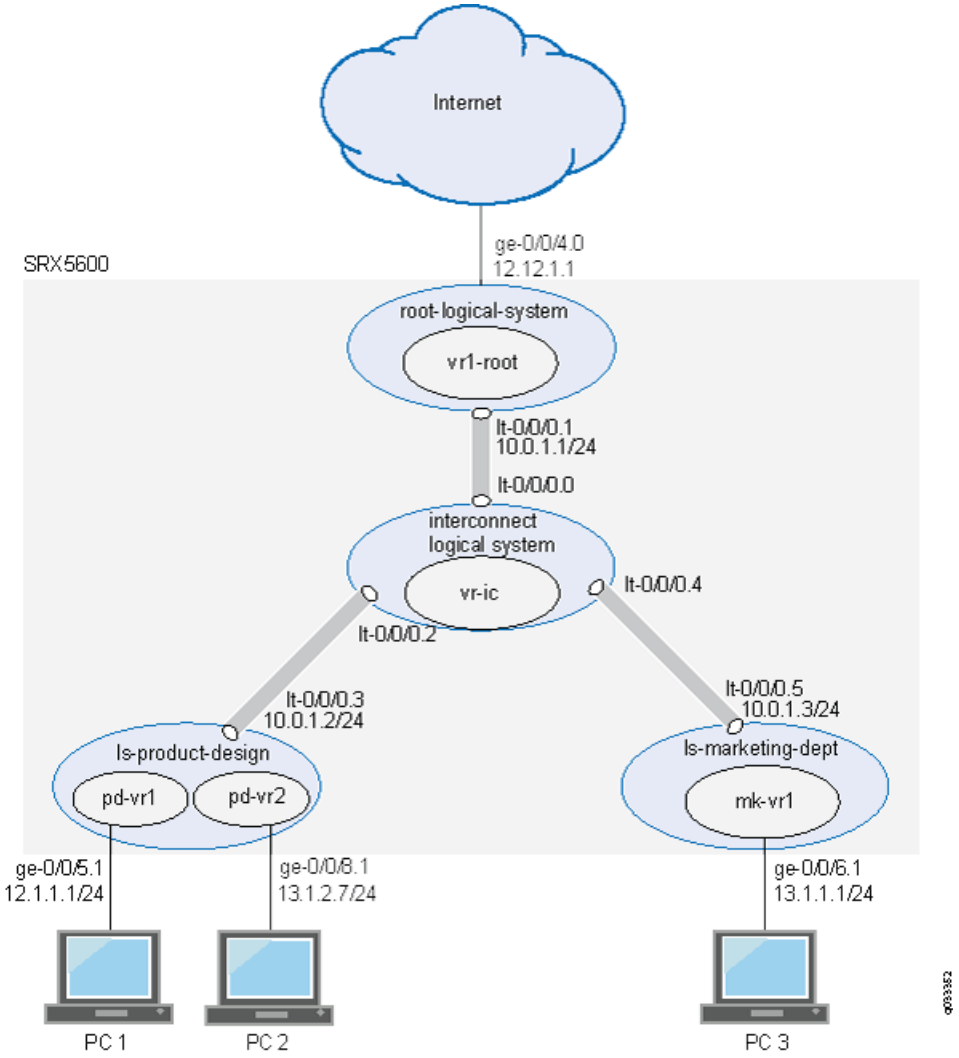
  Because the interconnect logical system acts as a virtual switch, it is configured as a virtual private LAN service (VPLS) routing instance type. The interconnect logical system's lt-0/0/0 interfaces are configured with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the master and user logical systems are configured with Ethernet as the encapsulation type.

  - lt-0/0/0.0 connects to lt-0/0/0.1 on the root logical system.
  - lt-0/0/0.2 connects to lt-0/0/0.3 on the ls-product-design logical system.

  - lt-0/0/0.4 connects to lt-0/0/0.5 on the ls-marketing-dept logical system.
  - lt-0/0/0.6 connects to lt-0/0/0.7 on the ls-accounting-dept logical system.
- For the master logical system, called root-logical-system, the example configures ge-0/0/4.0 and assigns it to the vr1-root routing instance. The example configures lt-0/0/0.1 to connect to lt-0/0/0.0 on the interconnect logical system and assigns it to the vr1-root routing instance. The example configures static routes to allow for communication with other logical systems and assigns them to the vr1-root routing instance.
- For the ls-product-design logical system, the example configures lt-0/0/0.3 to connect to lt-0/0/0.2 on the interconnect logical system.
- For the ls-marketing-dept logical system, the example configures lt-0/0/0.5 to connect to lt-0/0/0.4 on the interconnect logical system.
- For the ls-accounting-dept logical system, the example configures lt-0/0/0.7 to connect to lt-0/0/0.6 on the interconnect logical system.

Figure 4 on page 49 shows the topology for this deployment including virtual routers and their interfaces for all logical systems.

Figure 4: Configuring Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers



Configuration

This topic explains how to configure interfaces for logical systems.

- Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System on page 49
- Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System on page 51
- Configuring Logical Tunnel Interfaces for the User Logical Systems on page 53

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect 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 logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 0 encapsulation
    ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 2 encapsulation
    ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 4 encapsulation
    ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 6 encapsulation
    ethernet-vpls
set logical-systems interconnect-logical-system interfaces lt-0/0/0 unit 6 peer-unit 7
set logical-systems interconnect-logical-system routing-instances vr-ic instance-type
    vpls
set logical-systems interconnect-logical-system routing-instances vr-ic interface
    lt-0/0/0.0
set logical-systems interconnect-logical-system routing-instances vr-ic interface
    lt-0/0/0.2
set logical-systems interconnect-logical-system routing-instances vr-ic interface
    lt-0/0/0.4
set logical-systems interconnect-logical-system routing-instances vr-ic interface
    lt-0/0/0.6
```

Step-by-Step Procedure

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

To configure the interconnect system lt-0/0/0 interfaces and routing instances:

1. Configure the lt-0/0/0 interfaces.

```
[edit logical-systems]
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 0 encapsulation
    ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 0 peer-unit 1
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 2 encapsulation
    ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 2 peer-unit 3
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 4 encapsulation
    ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 4 peer-unit 5
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 6 encapsulation
    ethernet-vpls
user@host# set interconnect-logical-system interfaces lt-0/0/0 unit 6 peer-unit 7
```

2. Configure the routing instance for the interconnect logical system and add its lt-0/0/0 interfaces to it.

```
[edit logical-systems]
user@host# set interconnect-logical-system routing-instances vr-ic instance-type
    vpls
user@host# set interconnect-logical-system routing-instances vr-ic interface
    lt-0/0/0.0
```

```
user@host# set interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.2
user@host# set interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.4
user@host# set interconnect-logical-system routing-instances vr-ic interface
  lt-0/0/0.6
```

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

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

```
user@host# show logical-systems interconnect-logical-system
  interfaces {
    lt-0/0/0 {
      unit 0 {
        encapsulation ethernet-vpls;
        peer-unit 1;
      }
      unit 2 {
        encapsulation ethernet-vpls;
        peer-unit 3;
      }
      unit 4 {
        encapsulation ethernet-vpls;
        peer-unit 5;
      }
      unit 6 {
        encapsulation ethernet-vpls;
        peer-unit 7;
      }
    }
  }
    routing-instances {
      vr-ic {
        instance-type vpls;
        interface lt-0/0/0.0;
        interface lt-0/0/0.2;
        interface lt-0/0/0.4;
        interface lt-0/0/0.6;
      }
    }
```

Configuring Interfaces, a Routing Instance, and Static Routes for the Master 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-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 600
```

```
set interfaces ge-0/0/4 unit 0 family inet address 12.12.1.1/24
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/6 vlan-tagging
set interfaces ge-0/0/7 vlan-tagging
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 10.0.1.1/24
set routing-instances vr1-root instance-type virtual-router
set routing-instances vr1-root interface ge-0/0/4.0
set routing-instances vr1-root interface lt-0/0/0.1
set routing-instances vr1-root routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
set routing-instances vr1-root routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
set routing-instances vr1-root routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
```

Step-by-Step Procedure

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

To configure the master logical system interfaces:

1. Configure the master (root) logical and lt-0/0/0.1 interfaces.

```
[edit interfaces]
user@host# set ge-0/0/4 vlan-tagging
user@host# set ge-0/0/4 unit 0 vlan-id 600
user@host# set ge-0/0/4 unit 0 family inet address 12.12.1.1/24
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 10.0.1.1/24
```

2. Configure the interfaces for other logical systems to support VLAN tagging.

```
[edit interfaces]
user@host# set ge-0/0/5 vlan-tagging
user@host# set ge-0/0/6 vlan-tagging
user@host# set ge-0/0/7 vlan-tagging
```

3. Configure a routing instance for the master logical system, assign its interfaces to it, and configure static routes for it.

```
[edit routing-instances]
user@host# set vr1-root instance-type virtual-router
user@host# set vr1-root interface ge-0/0/4.0
user@host# set vr1-root interface lt-0/0/0.1
user@host# set vr1-root routing-options static route 12.1.1.0/24 next-hop 10.0.1.2
user@host# set vr1-root routing-options static route 13.1.1.0/24 next-hop 10.0.1.3
user@host# set vr1-root routing-options static route 14.1.1.0/24 next-hop 10.0.1.4
```

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.

```
[edit]
user@host# show interfaces
  ge-0/0/4 {
    vlan-tagging;
```

```
        unit 0 {
          vlan-id 600;
          family inet {
            address 12.12.1.1/24;
          }
        }
      }
        ge-0/0/5 {
          vlan-tagging;
        }
        ge-0/0/6 {
          vlan-tagging;
        }
        ge-0/0/7 {
          vlan-tagging;
        }
        lt-0/0/0 {
          unit 1 {
            encapsulation ethernet;
            peer-unit 0;
            family inet {
              address 10.0.1.1/24;
            }
          }
        }

[edit]
user@host# show routing-instances
  vr1-root {
    instance-type virtual-router;
    interface ge-0/0/4.0;
    interface lt-0/0/0.1;
    routing-options {
      static {
        route 14.1.1.0/24 next-hop 10.0.1.4;
        route 12.1.1.0/24 next-hop 10.0.1.2;
        route 13.1.1.0/24 next-hop 10.0.1.3;
      }
    }
  }
```

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

Configuring Logical Tunnel Interfaces for the User Logical Systems

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 logical-systems ls-product-design interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems ls-product-design interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems ls-product-design interfaces lt-0/0/0 unit 3 family inet address
  10.0.1.2/24
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 peer-unit 4
```

```
set logical-systems ls-marketing-dept interfaces lt-0/0/0 unit 5 family inet address
  10.0.1.3/24
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 encapsulation ethernet
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 peer-unit 6
set logical-systems ls-accounting-dept interfaces lt-0/0/0 unit 7 family inet address
  10.0.1.4/24
```

Step-by-Step Procedure

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

1. Configure the lt-0/0/0 interface for the first user logical system:

```
[edit logical-systems]
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 encapsulation ethernet
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 peer-unit 2
user@host# set ls-product-design interfaces lt-0/0/0 unit 3 family inet address
  10.0.1.2/24
```

2. Configure the lt-0/0/0 interface for the second user logical system.

```
[edit logical-systems]
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 encapsulation ethernet
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 peer-unit 4
user@host# set ls-marketing-dept interfaces lt-0/0/0 unit 5 family inet address
  10.0.1.3/24 face
```

3. Configure the lt-0/0/0 interface for the third user logical system.

```
[edit logical-systems]
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 encapsulation ethernet
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 peer-unit 6
user@host# set ls-accounting-dept interfaces lt-0/0/0 unit 7 family inet address
  10.0.1.4/24
```

Results

From configuration mode, confirm your configuration by entering the **show logical-systems ls-product-design interfaces lt-0/0/0**, **show logical-systems ls-marketing-dept interfaces lt-0/0/0** , and **show logical-systems ls-accounting-dept interfaces lt-0/0/0** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host#  show logical-systems ls-product-design interfaces lt-0/0/0

lt-0/0/0 {
  unit 3 {
    encapsulation ethernet;
    peer-unit 2;
    family inet {
      address 10.0.1.2/24;
    }
  }
}
user@host# show logical-systems ls-marketing-dept interfaces lt-0/0/0
  lt-0/0/0 {
    unit 5 {
      encapsulation ethernet;
      peer-unit 4;
```

```
        family inet {
          address 10.0.1.3/24;
        }
      }
    }
  }
user@host# show logical-systems ls-accounting-dept interfaces lt-0/0/0
lt-0/0/0 {
  unit 7 {
    encapsulation ethernet;
    peer-unit 6;
    family inet {
      address 10.0.1.4/24;
    }
  }
}
```

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 That the Static Routes Configured for the Master Administrator Are Correct on page 55

Verifying That the Static Routes Configured for the Master Administrator Are Correct

Purpose Verify if you can send data from the master logical system to the other logical systems.

Action From operational mode, use the **ping** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 10

Understanding CPU Allocation and Control

When device CPU utilization is low, logical systems can acquire and use CPU resources above their allocated reserve quotas as long as the system-wide utilization remains within a stable range. CPU utilization on a device should never reach 100 percent because a device running at 100 percent CPU utilization might be slow to respond to management or system events or be unable to handle traffic bursts.

CPU resources are used on a first-come first-served basis. Without controls, logical systems can compete for CPU resources and drive CPU utilization up to 100 percent. You

cannot rely on the configuration of static resources, such as security policies and zones, to directly control CPU usage because a logical system with small numbers of static resources allocated could still consume a large amount of CPU. Instead, the master administrator can enable CPU resource control and configure CPU utilization parameters for logical systems.

NOTE: Only the master administrator can enable CPU control and configure CPU utilization parameters. User logical system administrators can use the **show system security-profile cpu** command to view CPU utilization for their logical systems.

This topic includes the following sections:

CPU Control

The master administrator enables CPU control with the **cpu-control** configuration statement at the [**edit system security-profile resources**] hierarchy level.

NOTE: The resources security profile is a special security profile that contains global settings that apply to all logical systems in the device. Other security profiles configured by the master administrator are bound to specific logical systems.

When CPU control is enabled, the master administrator can then configure the following CPU utilization parameters:

- A reserved CPU quota is the percentage of CPU utilization that is guaranteed for a logical system.
- The CPU control target is the upper limit, in percent, for system-wide CPU utilization on the device under normal operating conditions.

Reserved CPU Utilization Quota for Logical Systems

A configured reserved CPU quota guarantees that a specified percentage of CPU is always available to a logical system. During runtime, CPU utilization by each logical system is measured every two seconds. The reserved CPU quota is used to calculate the amount of CPU each logical system can use based on the runtime utilization.

The master administrator specifies the reserved CPU quota in a logical system security profile with the **cpu reserved** configuration statement at the [**edit system security-profile**

profile-name] hierarchy level. The security profile is bound to one or more logical systems. Unlike other resources that are allocated to a logical system in a security profile, no maximum allowed quota can be configured for CPU utilization.

The Junos OS software checks to ensure that the sum of reserved CPU quotas for all logical systems on the device is less than 90 percent of the CPU control target value. If CPU control is enabled and reserved CPU quotas are not configured, the default reserved CPU quota for the master logical system is 1 percent and the default reserved CPU quota for user logical systems is 0 percent. The master administrator can configure reserved CPU quotas even if CPU control is not enabled. The master administrator can enable or disable CPU control without changing security profiles.

CAUTION: **The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota because traffic loss could occur.**

CPU Control Target

CPU control target is the upper limit, in percent, for CPU utilization on the device under normal operating conditions. If CPU utilization on the device surpasses the configured target value, the Junos OS software initiates controls to bring CPU utilization between the target value and 90 percent of the target value. For example, if the CPU control target value is 80 and CPU utilization on the device surpasses 80 percent, then controls are initiated to bring CPU utilization within the range of 72 (90 percent of 80) and 80 percent.

During runtime, CPU utilization by each logical system is measured every two seconds. Dropping packets reduces the CPU usage for a logical system. If the CPU usage of a logical system exceeds its quota, CPU utilization control drops the packets received on that logical system. The packet drop rate is calculated every two seconds based on CPU utilization of all logical systems.

The master administrator configures the CPU control target with the **cpu-control-target** configuration statement at the [**edit system security-profile resources**] hierarchy level. A stable level of CPU utilization should be relatively close to 100 percent but allow for bursts in CPU utilization. The master administrator should configure the CPU control target level based on an understanding of the usage pattern of the logical system's deployment on the device.

CPU control must be enabled for the Junos OS software to control CPU usage. If the master administrator enables CPU control without specifying a CPU control target value, the default CPU control target is 80 percent.

Shared CPU Resources and CPU Quotas

The sum of the reserved CPU quotas for all logical systems on the device must be less than 90 percent of the CPU control target; the difference is called the *shared CPU resource*. The shared CPU resource is dynamically allocated among the logical systems that need additional CPU. This means that a logical system can use more CPU than its reserved CPU quota.

The *CPU quota* for a logical system is the sum of its reserved CPU quota and its portion of the shared CPU resource. If multiple logical systems need more CPU resources, they split the shared CPU resource based on the relative weights of their reserved CPU quotas. Logical systems with larger reserved CPU quotas receive larger portions of the shared CPU resource. The goal for CPU control is to keep the actual CPU utilization of a logical system at its CPU quota. If a logical system's CPU needs are greater than its CPU quota, packets are dropped for that logical system.

The following scenarios illustrate CPU control for logical systems. In each scenario, the CPU control target value is 80, which means that CPU controls will keep the maximum system-wide CPU utilization between 72 and 80 percent. The reserved CPU quotas for the logical systems are configured as follows: master and lsys1 logical systems are 10 percent each and the lsys2 logical system is 5 percent.

CPU Utilization Scenario 1

In this scenario, each of the three logical systems needs 40 percent of CPU. Table 5 on page 58 shows the CPU quotas for each logical system. Because the CPU needed by each logical system is greater than its CPU quota, packets are dropped for each logical system.

Table 5: CPU Utilization Scenario 1

Logical System	Needed CPU	CPU Quotas	Packets Dropped?
master	40%	28.8%	Yes
lsys1	40%	28.8%	Yes
lsys2	40%	14.4%	Yes

CPU Utilization Scenario 2

In this scenario, the master logical system needs 25 percent of CPU while the two user logical systems need 40 percent. Table 6 on page 58 shows the CPU quota for the master logical system is equal to the CPU it needs, so no packets are dropped for the master logical system and CPU control monitors the CPU utilization of the master logical system. Packets are dropped for lsys1 and lsys2.

Table 6: CPU Utilization Scenario 2

Logical System	Needed CPU	CPU Quotas	Packets Dropped?
master	25%	25%	No
lsys1	40%	31.3%	Yes
lsys2	40%	15.6%	Yes

CPU Utilization Scenario 3

In this scenario, the master and lsys2 logical systems need 5 percent and 3 percent of CPU, respectively, while lsys1 needs 40 percent. Table 7 on page 59 shows system-wide CPU utilization is 48 percent, which is less than 72 percent (90 percent of the CPU control target), so no packets are dropped and CPU control monitors all logical systems.

Table 7: CPU Utilization Scenario 3

Logical System	Needed CPU	CPU Quota	Packets Dropped?
master	5%	5%	No
lsys1	40%	40%	No
lsys2	3%	3%	No

Monitoring CPU Utilization

CPU utilization can be monitored by either the master administrator or the user logical system administrators. The master administrator can monitor CPU utilization for the master logical system, a specified user logical system, or all logical systems. User logical system administrators can only monitor CPU utilization for their logical system.

The **show system security-profile cpu** command shows the usage and drop rate in addition to the reserved CPU quota configured for the logical system. During runtime, CPU utilization by each logical system is measured every two seconds. The usage and drop rates displayed are the values at the interval prior to when the **show** command is run. If the **detail** option is not specified, the utilization of the central point (CP) and the average utilization of all services processing units (SPUs) is shown. The **detail** option displays the CPU utilization on each SPU.

The CPU utilization log file **lsys-cpu-utilization-log** contains utilization data for all logical systems on the device. Only the master administrator can view the log file with the **show log lsys-cpu-utilization-log** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems Security Profiles on page 34
- Example: Configuring CPU Utilization on page 59

Example: Configuring CPU Utilization

The master administrator can enable CPU control and configure CPU utilization parameters. This example shows how to enable CPU utilization control and configure CPU utilization quotas and a control target.

- Requirements on page 60
- Overview on page 60

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.
- Bind security profiles to the master logical system and user logical systems configured on the device. See "Example: Configuring Logical Systems Security Profiles" on page 40.

Overview

In this example, you enable CPU control and set the CPU control target to be 85 percent. You allocate reserved CPU quotas to the logical systems shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26. The logical systems are bound to the security profiles shown in Table 8 on page 60 and are assigned the reserved CPU quotas in the security profiles.

Table 8: Logical Systems, Security Profiles, and Reserved CPU Quotas

Logical System	Security Profile	Reserved CPU Quotas
root-logical-system (master)	master-profile	2 percent
ls-product-design	ls-design-profile	2 percent
ls-marketing-dept, ls-accounting-dept	ls-accnt-mrkt-profile	1 percent

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 system security-profile resources cpu-control
set system security-profile resources cpu-control-target 85
set system security-profile master-profile cpu reserved 2
set system security-profile ls-design-profile cpu reserved 2
set system security-profile ls-accnt-mrkt-profile cpu reserved 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 in the *Junos OS CLI User Guide*.

To configure CPU utilization control parameters:

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

```
[edit]
admin@host> configure
admin@host#
```

2. Enable CPU control.

```
[edit system security-profile resources]
admin@host# set cpu-control
```

3. Configure the CPU control target.

```
[edit system security-profile resources]
admin@host# set cpu-control-target 85
```

4. Configure the reserved CPU quotas in the security profiles.

```
[edit system]
admin@host# set security-profile security-profile master-profile cpu reserved 2
admin@host# set security-profile security-profile ls-design-profile cpu reserved 2
admin@host# set security-profile security-profile ls-accnt-mrkt-profile cpu reserved
  1
```

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

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]
admin@host# show system security-profile
  resources {
    cpu-control;
    cpu-control-target 85;
  }
    ls-accnt-mrkt-profile {
      ...
      cpu {
        reserved 1;
      }
      logical-system [ ls-marketing-dept ls-accounting-dept ];
    }
    ls-design-profile {
      ...
      cpu {
        reserved 2;
      }
      logical-system ls-product-design;
    }
    master-profile {
      ...
      cpu {
        reserved 2;
      }
      logical-system root-logical-system;
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying CPU Utilization on page 62

Verifying CPU Utilization

Purpose Display the configured reserved CPU quota, the actual CPU usage, and the drop rate.

Action From operational mode, enter the **show system security-profile cpu logical-system all** command.

```
admin@host> show system security-profile cpu logical-system all
CPU control: TRUE
CPU control target: 85.00%
logical system name    profile name    CPU name    usage(%)    reserved(%)
drop rate(%)
root-logical-system    master-profile CP              0.10%          2.00%
     0.00%
root-logical-system    master-Profile SPU             0.25%          2.00%
     0.00%
ls-product-design      ls-design-profile CP           0.53%          2.00%
     0.00%
ls-product-design      ls-design-profile SPU          0.26%          2.00%
     0.00%
ls-marketing-dept      ls-acct-mrkt-profile CP        0.10%          1.00%
     0.00%
ls-marketing-dept      ls-acct-mrkt-profile SPU       0.15%          1.00%
     0.00%
ls-accounting-dept     ls-acct-mrkt-profile CP        0.23%          1.00%
     0.00%
ls-accounting-dept     ls-acct-mrkt-profile SPU       0.34%          1.00%
     0.00%
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding CPU Allocation and Control on page 55
- Understanding Logical Systems Security Profiles on page 34

Example: Configuring OSPF Routing Protocol for the Master Logical System

This example shows how to configure OSPF for the master logical system.

- Requirements on page 63
- Overview on page 63
- Configuration on page 63
- Verification on page 65

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Example: Configuring a Root Password for the Device" on page 26.
- Configure logical interfaces ge-0/0/4.0 and lt-0/0/0.1 for the master logical system and assign them to the vr1-root routing instance. See "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for User Logical Systems" on page 47.

Overview

In this example, you configure OSPF for the master logical system, called root-logical-system, shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26.

This example enables OSPF routing on the ge-0/0/4.0 and lt-0/0/0.1 interfaces in the master logical system. You configure the following routing policies to export routes from the Junos OS routing table into OSPF in the vr1-root 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 vr1-root protocols ospf export ospf-redist-direct
set routing-instances vr1-root protocols ospf export ospf-redist-static
set routing-instances vr1-root protocols ospf export ospf-to-ospf
set routing-instances vr1-root protocols ospf area 0.0.0.1 interface ge-0/0/4.0
set routing-instances vr1-root protocols ospf area 0.0.0.1 interface lt-0/0/0.1
```

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 in the *Junos OS CLI User Guide*.

To configure OSPF for the master logical system:

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

```
admin@host> configure
admin@host#
```

2. Create routing policies that accept routes.

```
[edit policy-options]
admin@host# set policy-statement ospf-redist-direct from protocol direct
admin@host# set policy-statement ospf-redist-direct then accept
admin@host# set policy-statement ospf-redist-static from protocol static
admin@host# set policy-statement ospf-redist-static then accept
admin@host# set policy-statement ospf-to-ospf from protocol ospf
admin@host# set policy-statement ospf-to-ospf then accept
```

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

```
[edit routing-instances]
admin@host# set vr1-root protocols ospf export ospf-redist-direct
admin@host# set vr1-root protocols ospf export ospf-redist-static
admin@host# set vr1-root protocols ospf export ospf-to-ospf
```

4. Enable OSPF on the logical interfaces.

```
[edit routing-instances]
admin@host# set vr1-root protocols ospf area 0.0.0.1 interface ge-0/0/4.0
admin@host# set vr1-root protocols ospf area 0.0.0.1 interface lt-0/0/0.1
```

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]
  admin@host# 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]
  admin@host# show routing-instances
    vr1-root {
      ...
      protocols {
        ospf {
          export [ ospf-redist-direct ospf-to-ospf ospf-redist-static ];
          area 0.0.0.1 {
            interface lt-0/0/0.1;
            interface ge-0/0/4.0;
          }
        }
      }
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying OSPF Interfaces on page 65
- Verifying OSPF Neighbors on page 65
- Verifying OSPF Routes on page 65

Verifying OSPF Interfaces

Purpose Verify OSPF-enabled interfaces.

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

```
admin@host> show ospf interface instance vr1-root
Interface           State   Area            DR ID           BDR ID          Nbrs
lt-0/0/0.1          DR      0.0.0.0         10.0.1.1        0.0.0.0            0
ge-0/0/4.0          DR      0.0.0.1         10.0.1.1        0.0.0.0            0
```

Verifying OSPF Neighbors

Purpose Verify OSPF neighbors.

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

```
admin@host> show ospf neighbor instance vr1-root
Address   Interface  State   ID      Pri Dead
10.0.1.2  plt0.3    Full    0.0.0.0    128   39
```

Verifying OSPF Routes

Purpose Verify OSPF routes.

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

```
admin@host> show ospf route instance vr1-root
```

```
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-0/0/0.1
12.12.1.0/24        Intra Network    IP            1 ge-0/0/4.0
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Interfaces and Routing Instances on page 88
- Example: Configuring OSPF Routing Protocol for a User Logical System on page 91
- OSPF Configuration Overview in the *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- Verifying an OSPF Configuration in the *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

Example: Configuring Security Features for the Master Logical System

This example shows how to configure security features, such as zones, policies, and firewall authentication, for the master logical system.

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Example: Configuring a Root Password for the Device" on page 26.
- Use the **show system security-profile** command to see the resources allocated to the master logical system. See the *Junos OS CLI Reference*.
- Configure logical interfaces for the master logical system. See "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Master and Interconnect Logical Systems and Logical Tunnel Interfaces for User Logical Systems" on page 47.
- Configure the access profile ldap1 in the master logical system. The ldap1 access profile is used for Web authentication of firewall users. See "Example: Configuring Access Profiles" on page 108.

Overview

In this example, you configure security features for the master logical system, called root-logical-system, shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26. This example configures the security features described in Table 9 on page 67.

Table 9: root-logical-system Security Feature Configuration

Feature	Name	Configuration Parameter
Zones	ls-root-trust	Bind to interface ge-0/0/4.0.
	ls-root-untrust	Bind to interface lt-0/0/0.1
Address books	root-internal	• Address masters: 12.12.1.0/24 • Attach to zone ls-root-trust
	root-external	• Address design: 12.1.1.0/24 • Address accounting: 14.1.1.0/24 • Address marketing: 13.1.1.0/24 • Address set userlsys: design, accounting, marketing • Attach to zone ls-root-untrust
Security policies	permit-to-userlsys	Permit the following traffic: • From zone: ls-root-trust • To zone: ls-root-untrust • Source address: masters • Destination address: userlsys • Application: any
	permit-authorized-users	Permit the following traffic: • From zone: ls-root-untrust • To zone: ls-root-trust • Source address: userlsys • Destination address: masters • Application: junos-http, junos-https
Firewall authentication		• Web authentication • Authentication success banner “WEB AUTH LOGIN SUCCESS” • Default access profile ldap1
HTTP daemon		Activate on interface ge-0/0/4.0

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 root-internal address masters 12.12.1.0/24
set security address-book root-internal attach zone ls-root-trust
set security address-book root-external address design 12.1.1.0/24
set security address-book root-external address accounting 14.1.1.0/24
set security address-book root-external address marketing 13.1.1.0/24
set security address-book root-external address-set userlsys address design
```

```
set security address-book root-external address-set userlsys address accounting
set security address-book root-external address-set userlsys address marketing
set security address-book root-external attach zone ls-root-untrust
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match source-address masters
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match destination-address userlsys
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys match application any
set security policies from-zone ls-root-trust to-zone ls-root-untrust policy
  permit-to-userlsys then permit
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match source-address userlsys
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match destination-address masters
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match application junos-http
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users match application junos-https
set security policies from-zone ls-root-untrust to-zone ls-root-trust policy
  permit-authorized-users then permit firewall-authentication web-authentication
set security zones security-zone ls-root-trust interfaces ge-0/0/4.0
set security zones security-zone ls-root-untrust interfaces lt-0/0/0.1
set system services web-management http interface ge-0/0/4.0
set access firewall-authentication web-authentication default-profile ldap1
set access firewall-authentication web-authentication banner success "WEB AUTH
  LOGIN SUCCESS"
```

Step-by-Step Procedure

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

To configure zones and policies for the master logical system:

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

   ```
   admin@host> configure
   admin@host#
   ```

2. Create security zones and assign interfaces to each zone.

   ```
   [edit security zones]
   admin@host# set security-zone ls-root-trust interfaces ge-0/0/4.0
   admin@host# set security-zone ls-root-untrust interfaces lt-0/0/0.1
   ```

3. Create address book entries.

   ```
   [edit security]
   admin@host# set address-book root-internal address masters 12.12.1.0/24
   admin@host# set address-book root-external address design 12.1.1.0/24
   admin@host# set address-book root-external address accounting 14.1.1.0/24
   admin@host# set address-book root-external address marketing 13.1.1.0/24
   admin@host# set address-book root-external address-set userlsys address design
   admin@host# set address-book root-external address-set userlsys address
     accounting
   ```

```
admin@host# set address-book root-external address-set userlsys address
  marketing
```

4. Attach address books to zones.

```
[edit security]
admin@host# set address-book root-internal attach zone ls-root-trust
admin@host# set address-book root-external attach zone ls-root-untrust
```

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

```
[edit security policies from-zone ls-root-trust to-zone ls-root-untrust]
admin@host# set policy permit-to-userlsys match source-address masters
admin@host# set policy permit-to-userlsys match destination-address userlsys
admin@host# set policy permit-to-userlsys match application any
admin@host# set policy permit-to-userlsys then permit
```

6. Configure a security policy that authenticates traffic from the ls-root-untrust zone to the ls-root-trust zone.

```
[edit security policies from-zone ls-root-untrust to-zone ls-root-trust]
admin@host# set policy permit-authorized-users match source-address userlsys
admin@host# set policy permit-authorized-users match destination-address masters
admin@host# set policy permit-authorized-users match application junos-http
admin@host# set policy permit-authorized-users match application junos-https
admin@host# set policy permit-authorized-users then permit firewall-authentication
  web-authentication
```

7. Configure the Web authentication access profile and define a success banner.

```
[edit access]
admin@host# set firewall-authentication web-authentication default-profile ldap1
admin@host# set firewall-authentication web-authentication banner success “WEB
  AUTH LOGIN SUCCESS”
```

8. Activate the HTTP daemon on the device.

```
[edit system]
admin@host# set services web-management http interface ge-0/0/4.0
```

Results From configuration mode, confirm your configuration by entering the **show security**, **show access**, and **show system services** 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]
admin@host# show security
...
address-book {
  root-internal {
    address masters 12.12.1.0/24;
    attach {
      zone ls-root-trust;
    }
```

```
    }
    root-external {
      address design 12.1.1.0/24;
      address accounting 14.1.1.0/24;
      address marketing 13.1.1.0/24;
      address-set userlsys {
        address design;
        address accounting;
        address marketing;
      }
      attach {
        zone ls-root-untrust;
      }
    }
  }
    policies {
      from-zone ls-root-trust to-zone ls-root-untrust {
        policy permit-to-userlsys {
          match {
            source-address masters;
            destination-address userlsys;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone ls-root-untrust to-zone ls-root-trust {
        policy permit-authorized-users {
          match {
            source-address userlsys;
            destination-address masters;
            application [ junos-http junos-https ];
          }
          then {
            permit {
              firewall-authentication {
                web-authentication;
              }
            }
          }
        }
      }
    }
    zones {
      security-zone ls-root-trust {
        interfaces {
          ge-0/0/4.0;
        }
      }
      security-zone ls-root-untrust {
        interfaces {
          lt-0/0/0.1;
        }
      }
```

```
    }
[edit]
admin@host# show access
...
firewall-authentication {
    web-authentication {
        default-profile ldap1;
        banner {
            success "WEB AUTH LOGIN SUCCESS";
        }
    }
}
[edit]
admin@host# show system services
web-management {
    http {
        interface ge-0/0/4.0;
    }
}
```

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 71

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Zones on page 95
- Understanding Logical System Security Policies on page 102
- Understanding Logical System Firewall Authentication on page 107

Example: Configuring an IDP Policy for the Master Logical System

This example shows how to configure an IDP policy in a master logical system.

- Requirements on page 72
- Overview on page 72
- Configuration on page 73
- Verification on page 77

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.
- Read "IDP in Logical Systems Overview" on page 127.
- Use the **show system security-profile** command to see the resources allocated to the master logical system. See the *Junos OS CLI Reference*.

Overview

In this example you configure a custom attack that is used in an IDP policy. The IDP policy is specified in a security profile that is applied to the master logical system. IDP is then enabled in a security policy configured in the master logical system.

You configure the features described in Table 10 on page 72.

Table 10: IDP Configuration for the Master Logical System

Feature	Name	Configuration Parameters

Custom attack	http-bf	• Severity critical
		• Detect three attacks between source and destination addresses of sessions.
		• Stateful signature attack type with the following characteristics:
		  ◦ location http-url-parsed
		  ◦ pattern .*juniper.*
		  ◦ client to server traffic

IPS rulebase policy	root-idp-policy	Match: • application default • http-bf custom attacks Action: • drop-connection • notification log-attacks
Logical system security profile	master-profile (previously configured and applied to root-logical-system)	Add IDP policy root-idp-policy.
Security policy	enable-idp	Enable IDP in a security policy that matches any traffic from the lsys-root-untrust zone to the lsys-root-trust zone.

NOTE: A logical system can have only one active IDP policy at a time. To specify the active IDP policy for the master logical system, the master administrator can reference the IDP policy in the security profile that is bound to the master logical system as shown in this example. Alternatively, the master administrator can use the **active-policy** configuration statement at the **[edit security idp]** hierarchy level.

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.

Configuration

Configuring a Custom Attack

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 security idp custom-attack http-bf severity critical
set security idp custom-attack http-bf time-binding count 3
set security idp custom-attack http-bf time-binding scope peer
set security idp custom-attack http-bf attack-type signature context http-url-parsed
set security idp custom-attack http-bf attack-type signature pattern .*juniper.*
set security idp custom-attack http-bf attack-type signature direction client-to-server
```

Step-by-Step Procedure

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

To configure a custom attack object:

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

   ```
   [edit]
   admin@host> configure
   admin@host#
   ```

2. Create the custom attack object and set the severity level.

   ```
   [edit security idp]
   admin@host# set custom-attack http-bf severity critical
   ```

3. Configure attack detection parameters.

   ```
   [edit security idp]
   ```

```
admin@host# set custom-attack http-bf time-binding count 3
admin@host# set custom-attack http-bf time-binding scope peer
```

4. Configure stateful signature parameters.

```
[edit security idp]
admin@host# set custom-attack http-bf attack-type signature context
  http-url-parsed
admin@host# set custom-attack http-bf attack-type signature pattern .*juniper.*
admin@host# set custom-attack http-bf attack-type signature direction
  client-to-server
```

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

```
[edit]
admin@host# show security idp custom-attack http-bf
severity critical;
  time-binding {
    count 3;
    scope peer;
  }
    attack-type {
      signature {
        context http-url-parsed;
        pattern .*juniper.*;
        direction client-to-server;
      }
    }
```

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

Configuring an IDP Policy for the Master 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 security idp idp-policy root-idp-policy rulebase-ips rule 1 match application default
set security idp idp-policy root-idp-policy rulebase-ips rule 1 match attacks custom-attacks
  http-bf
set security idp idp-policy root-idp-policy rulebase-ips rule 1 then action drop-connection
set security idp idp-policy root-idp-policy rulebase-ips rule 1 then notification log-attacks
set system security-profile master-profile idp-policy lsys1-idp-policy
```

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

To configure an IDP policy:

1. Create the IDP policy and configure match conditions.

```
[edit security idp]
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 match application
  default
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 match attacks
  custom-attacks http-bf
```

2. Configure actions for the IDP policy.

```
[edit security idp]
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 then action
  drop-connection
admin@host# set idp-policy root-idp-policy rulebase-ips rule 1 then notification
  log-attacks
```

3. Add the IDP policy to the security profile.

```
[edit system security-profile master-profile]
admin@host# set idp-policy lsys1-idp-policy
```

Results From configuration mode, confirm your configuration by entering the **show security idp idp-policy root-idp-policy** and **show system security-profile master-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
admin@host# show security idp idp-policy root-idp-policy
  rulebase-ips {
    rule 1 {
      match {
        application default;
        attacks {
          custom-attacks http-bf;
        }
      }
      then {
        action {
          drop-connection;
        }
        notification {
          log-attacks;
        }
      }
    }
  }
admin@host# show system security-profile master-profile
...
idp-policy lsys1-idp-policy;
```

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

Enabling IDP in a Security Policy

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

Step-by-Step Procedure

To enable IDP in a security policy:

1. Create the security policy and configure match conditions.

```
[edit security policies from-zone lsys-root-untrust to-zone lsys-root-trust]
admin@host# set policy enable-idp match source-address any
admin@host# set policy enable-idp match destination-address any
admin@host# set policy enable-idp match application any
```

2. Enable IDP.

```
[edit security policies from-zone lsys-root-untrust to-zone lsys-root-trust]
admin@host# 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]
  admin@host# show security policies
  from-zone lsys-root-untrust to-zone lsys-root-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
  IDP attack statistics:
    Attack name                    #Hits
    http-bf                        1
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- IDP in Logical Systems Overview on page 127
- SRX Series Logical System Master Administrator Configuration Tasks Overview on page 23

Example: Configuring Application Firewall Services for a Master Logical System

This example describes how to configure application firewall services on the master, or root, logical system by a master administrator. Only the master administrator can configure, manage, and view configuration of the master logical system, in addition to all user logical systems.

After configuring application firewall rule sets and rules, the master administrator adds the application firewall rule set information to the security policy on the master logical system.

For information about configuring an application firewall within a security policy, see the *Junos OS Security Configuration Guide*.

Requirements

Before you begin:

- Verify that all interfaces, routing instances, and security zones have been configured on the master logical system.

  See "Example: Configuring Security Features for the Master Logical System" on page 66.

- Verify that application firewall resources (appfw-rule-set and appfw-rule) have been allocated in a security profile and bound to the master logical system through the

[**system security-profile**] command. For application firewall resources, a security profile configuration allows 0 to 10,000 rule sets and 0 to 10,000 rules.

NOTE: The master administrator allocates various global system resources through a security profile configuration which is then bound to the various logical systems on the device. The master administrator owns this function and configures the security profile for all user logical systems as well as the master logical system.

For more information, see "Understanding Logical Systems Security Profiles" on page 34.

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

  For information about master administrator role functions, see "Understanding the Master Logical System and the Master Administrator Role" on page 8.

Overview

In this example you create application firewall services on the master logical system, called root-logical-system shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26.

This example creates the following application firewall configuration:

- Rule set, root-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, root-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 logical-systems root-logical-system security application-firewall rule-sets root-rs1
    rule r1 match dynamic-application junos:TELNET
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
    rule r1 then permit
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
    rule r2 match dynamic-application-group junos:web
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
    rule r2 then permit
set logical-systems root-logical-system security application-firewall rule-sets root-rs1
    default-rule deny
```

```
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  rule r1 match dynamic-application junos:facebook
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  rule r1 then deny
set logical-systems root-logical-system security application-firewall rule-sets root-rs2
  default-rule permit
```

Step-by-Step Procedure

To configure application firewall for a master logical system:

1. Log in to the master logical system as the master administrator. See "Example: Configuring a Root Password for the Device" on page 26 and enter configuration mode.

   ```
   admin@host> configure
   admin@host#
   ```

2. Configure an application firewall rule set for root-logical-system.

   ```
   [edit ]
   admin@host# set logical-systems security application-firewall rule-sets root-rs1
   ```

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

   ```
   [edit]
   admin@host# set logical-systems security application-firewall rule-sets root-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]
   admin@host# set logical-systems security application-firewall rule-sets root-rs1
     default-rule deny
   ```

5. Repeat these steps to configure another rule set, root-rs2, if desired.

Results

From configuration mode, confirm your configuration by entering the **show security application-firewall rule-sets** 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]
admin@host# show security application-firewall rule-sets all
...
  application-firewall {
    rule-sets root-rs1 {
      rule r1 {
        match {
          dynamic-application [junos:TELNET];
        }
        then {
          permit;
        }
```

```
    }
    default-rule {
      deny;
    }
  }
  rule-sets root-rs1 {
    rule r2 {
      match {
        dynamic-application-group [junos:web];
      }
      then {
        permit;
      }
    }
    rule-sets root-rs2 {
      rule r1 {
        match {
          dynamic-application [junos:FACEBOOK];
        }
        then {
          deny;
        }
      }
      default-rule {
        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 master logical system.

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

```
admin@host> show security application-firewall rule-set logical-system root-logical-system
rule-set all

Rule-set: root-rs1
    Logical system: root-logical-system
    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: root-rs1
```

```
    Logical system: root-logical-system
    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: root-rs2
    Logical system: root-logical-system
    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

- SRX Series Logical System Master Administrator Configuration Tasks Overview on page 23
- Understanding Logical Systems Security Profiles on page 34
- Understanding Logical System Application Firewall Services on page 137
- Example: Configuring Security Features for the Master Logical System on page 66

Example: Deleting an SRX Series Services Gateway Logical System

This example shows how to delete a logical system configured for an SRX Series Services Gateway device running logical systems. Only the master administrator can delete a logical system.

Requirements

The example uses an SRX5600 device running Junos OS with Logical Systems.

Alternatively, follow those instructions substituting your own configuration values.

Overview

This example shows how to delete a logical system, which you can do at any time. However, if you have configured the device to include the maximum number of logical systems that are supported you must first delete an existing logical system before you can add another one.

Deletion of a logical system is a simple procedure that includes these tasks:

- Remove from the logical system the security profile that is bound to it.

  Note that in this step you are not deleting the security profile—it might be used for other logical systems—but simply detaching it from the logical system that you intend to delete.

- Detach from the logical system any login classes that are associated with it.

  Removing them from the logical system does not delete the login classes.

- Delete the 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.

```
delete system security-profile ls-design-profile logical-system ls-product-design
delete system login class ls-design-admin logical-system ls-product-design
delete system login class ls-design-user logical-system ls-product-design
delete logical-system ls-product-design
```

Step-by-Step Procedure

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

To delete a logical system:

1. Determine that the logical system that you want to delete exists.

   ```
   [edit]
   user@host# show logical-systems ?
   interconnect-logical-system Logical system name
   ls-accounting-dept Logical system name
   ls-marketing-dept Logical system name
   ls-product-design Logical system name
   ```

2. Delete the security profile.

   a. Verify that security profile that you intend to detach from the logical system is bound to it.

      ```
      [edit]
      user@host# show system security-profile ls-design-profile
      logical-system [ ls-product-design ];
      ```

   b. Detach the security profile from the logical system.

      ```
      [edit]
      ```

```
user@host# delete system security-profile ls-design-profile logical-system
  ls-product-design
```

4. Delete the login classes.

   a. Display the login class and login user configurations for the user logical system administrator.

```
user@host> show configuration system login class ls-design-admin
logical-system ls-product-design;
permissions all;
user@host> show configuration system login user lsdesignadmin1
full-name lsdesignadmin1;
uid 2006;
class ls-design-admin;
authentication {
  encrypted-password "$1$VYfdRheI$CMSegr7Zi9RG4JNKa90iS/"; ##
    SECRET-DATA
  }
```

   b. Detach the login class for the administrator from the logical system.

```
[edit]
user@host# delete system login class ls-design-admin logical-system
  ls-product-design
```

   c. Display the login class and login user configurations for the user.

```
user@host> show configuration system login class ls-design-user
logical-system ls-product-design;
permissions view;
user@host> show configuration system login user lsdesignuser1
full-name lsdesignuser1
uid 2007;
class ls-design-user;
authentication {
  encrypted-password "$1$7tUK.xiD$NrODFcA1r5mRAFfP2ltXt0"; ##
    SECRET-DATA
  }
```

   d. Detach the login class for the user from the logical system.

```
user@host# delete system login class ls-design-user logical-system
  ls-product-design
```

5. Delete the logical system.

```
[edit]
user@host# delete logical-system ls-product-design
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems** command. In this case, the logical system that you deleted should not be included in displayed list of logical systems configured for the device. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show logical-systems
```

```
    interconnect-logical-system Logical system name
    ls-accounting-dept Logical system name
    interconnect-logical-system Logical system name
    ls-marketing-dept Logical system name
```

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 That the Correct Logical System and Its Profile and Attached Class Were Deleted on page 84

Verifying That the Correct Logical System and Its Profile and Attached Class Were Deleted

Purpose Verify if the logical system has been deleted using the show command described previously.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9
- Understanding Logical Systems for SRX Series Services Gateways on page 3

CHAPTER 3

User Logical System Configuration

- Example: Configuring AppTrack for a User Logical System on page 143
- Example: Configuring User Logical Systems on page 145

User Logical System Configuration Overview

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. See the *Junos OS CLI User Guide*.

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 options within each instance. See "Example: Configuring Interfaces and Routing Instances for a User Logical System" on page 89.

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 96.

   b. Configure screen options at the zone level. See "Example: Configuring Screen Options for a User Logical System" on page 100.

   c. Configure security policies between zones in the user logical system. See "Example: Configuring Security Policies in a User Logical System" on page 104.

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" on page 108.

   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 111.

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" on page 116.

   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 120.

f. Configure Network Address Translation (NAT). See "Example: Configuring Network Address Translation for a User Logical System" on page 124.

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" on page 132.

   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 134.

h. Display or clear application system cache (ASC) entries. See "Understanding Logical System Application Identification Services" on page 136.

i. Configure application firewall services on a user logical system. See "Understanding Logical System Application Firewall Services" on page 137 and "Example: Configuring Application Firewall Services for a User Logical System" on page 138.

j. Configure the AppTrack application tracking tool. See "Example: Configuring AppTrack for a User Logical System" on page 143.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring User Logical Systems on page 145
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9

Understanding Logical System Interfaces and Routing Instances

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Interfaces and Routing Instances for a User Logical System on page 89
- User Logical System Configuration Overview on page 86
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9
- *Junos OS Interfaces Configuration Guide for Security Devices*
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

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

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 86.
- Determine which logical interfaces and, optionally, which logical tunnel interfaces are allocated to your user logical system by the master administrator. The master administrator configures the logical tunnel interfaces. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.

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" on page 26.

This example configures the interfaces and routing instances described in Table 11 on page 89.

Table 11: 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 in the *Junos OS CLI User Guide*.

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#
   ```

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;
    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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- User Logical System Configuration Overview on page 86
- Understanding Logical System Interfaces and Routing Instances on page 88
- *Junos OS Interfaces Configuration Guide for Security Devices*
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

Example: Configuring OSPF Routing Protocol for a User Logical System

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 86.
- 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 89.

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" on page 26.

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 in the *Junos OS CLI User Guide*.

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
```

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;
          }
        }
      }
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying OSPF Interfaces on page 94
- Verifying OSPF Neighbors on page 94
- Verifying OSPF Routes on page 95

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Interfaces and Routing Instances on page 88
- Example: Configuring OSPF Routing Protocol for the Master Logical System on page 62
- OSPF Configuration Overview in the *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- Verifying an OSPF Configuration in the *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

Understanding Logical System Zones

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Zones for a User Logical System on page 96
- User Logical System Configuration Overview on page 86
- Understanding Logical Systems Security Profiles on page 34
- Understanding Logical System Interfaces and Routing Instances on page 88
- Security Zones and Interfaces Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Zones for a User Logical System

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 86.
- Use the **show system security-profile zones** command to see the zone resources allocated to the logical system. See the *Junos OS CLI Reference*.
- Logical interfaces for the user logical system must be configured. See "Example: Configuring Interfaces and Routing Instances for a User Logical System" on page 89.

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" on page 26.

This example creates the zones and address books described in Table 12 on page 97.

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: 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

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 in the *Junos OS CLI User Guide*.

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
   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 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
  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;
        }
      }
    }
```

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

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Zones on page 95
- User Logical System Configuration Overview on page 86

Understanding Logical System Screen Options

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Screen Options for a User Logical System on page 100
- User Logical System Configuration Overview on page 86
- Attack Detection and Prevention Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Screen Options for a User Logical System

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 86.
- Configure zones for the user logical system. See "Example: Configuring Zones for a User Logical System" on page 96.

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" on page 26.

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 13 on page 101.

Table 13: 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.

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 in the *Junos OS CLI User Guide*.

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

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

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- User Logical System Configuration Overview on page 86
- Understanding Logical System Screen Options on page 99

Understanding Logical System Security Policies

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 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Security Policies in a User Logical System on page 104
- Understanding Logical Systems Security Profiles on page 34
- User Logical System Configuration Overview on page 86
- Security Policies Overview in the *Junos OS Security Configuration Guide*
- Understanding Policy Application Timeout Configuration and Lookup in the *Junos OS Security Configuration Guide*

Example: Configuring Security Policies in a User Logical System

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 86.
- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system. See the *Junos OS CLI Reference*.
- Configure zones and address books. See "Example: Configuring Zones for a User Logical System" on page 96.

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" on page 26.

This example configures the security policies described in Table 14 on page 104.

Table 14: 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 in the *Junos OS CLI User Guide*.

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
   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 106

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Security Policies on page 102
- User Logical System Configuration Overview on page 86
- Troubleshooting Security Policies in the *Junos OS Security Configuration Guide*

Understanding Logical System Firewall Authentication

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Access Profiles on page 108
- Example: Configuring Firewall Authentication for a User Logical System on page 111
- User Logical System Configuration Overview on page 86
- Understanding Logical Systems Security Profiles on page 34
- Firewall User Authentication Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Access Profiles

The master administrator is responsible for configuring access profiles in the master logical system. This example shows how to configure access profiles.

- Requirements on page 109
- Overview on page 109
- Configuration on page 109

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.
- Read Firewall User Authentication Overview in the *Junos OS Security Configuration Guide*.

Overview

This example configures an access profile for LDAP authentication for logical system users. This example creates the access profile described in Table 15 on page 109.

NOTE: The master administrator creates the access profile.

Table 15: Access Profile Configuration

Name	Configuration Parameters

ldap1	• LDAP is used as the first (and only) authentication method.
	• Base distinguished name:
	  ◦ Organizational unit name (OU): people
	  ◦ Domain components (DC): example, com
	• A user's LDAP distinguished name is assembled through the use of a common name identifier, username, and base distinguished name. The common name identifier is user ID (UID).
	• The LDAP server address is 10.155.26.104 and is reached through port 389.

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.

NOTE: You must be logged in as the master administrator.

```
set access profile ldap1 authentication-order ldap
set access profile ldap1 ldap-options base-distinguished-name
  ou=people,dc=example,dc=com
set access profile ldap1 ldap-options assemble common-name uid
set access profile ldap1 ldap-server 10.155.26.104 port 389
```

Step-by-Step Procedure

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

To configure an access profile in the master logical system:

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

   ```
   admin@host> configure
   admin@host#
   ```

2. Configure an access profile and set the authentication order.

   ```
   [edit access profile ldap1]
   admin@host# set authentication-order ldap
   ```

3. Configure LDAP options.

   ```
   [edit access profile ldap1]
   admin@host# set ldap-options base-distinguished-name
     ou=people,dc=example,dc=com
   admin@host# set ldap-options assemble common-name uid
   ```

4. Configure the LDAP server.

   ```
   [edit access profile ldap1]
   admin@host# set ldap-server 10.155.26.104 port 389
   ```

Results

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

```
admin@host# show access profile ldap1
authentication-order ldap;
ldap-options {
  base-distinguished-name ou=people,dc=example,dc=com;
  assemble {
    common-name uid;
  }
}
  ldap-server {
    10.155.26.104 port 389;
  }
```

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

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Firewall Authentication for a User Logical System on page 111
- Understanding Logical System Firewall Authentication on page 107
- User Logical System Configuration Overview on page 86

Example: Configuring Firewall Authentication for a User Logical System

This example shows how to configure firewall authentication 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 86.
- Use the **show system security-profiles auth-entry** command to see the firewall authentication entries allocated to the logical system. See the *Junos OS CLI Reference*.
- Access profiles must be configured in the master logical system by the master administrator. See "Example: Configuring Access Profiles" on page 108.

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" on page 26.

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 16 on page 112.

NOTE: This example uses the access profile configured in "Example: Configuring Access Profiles" on page 108and address book entries configured in "Example: Configuring Zones for a User Logical System" on page 96.

Table 16: 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 104.) 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
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 in the *Junos OS CLI User Guide*.

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;
    }
  }
}
  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 114

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.

```
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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Access Profiles on page 108
- Understanding Logical System Firewall Authentication on page 107
- User Logical System Configuration Overview on page 86
- Example: Configuring Pass-Through Authentication in the *Junos OS Security Configuration Guide*

Understanding Route-Based VPN Tunnels in Logical Systems

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Route-Based IPsec VPNs in the *Junos OS Security Configuration Guide*
- User Logical System Configuration Overview on page 86
- Example: Configuring IKE and IPsec SAs for a VPN Tunnel on page 116
- Example: Configuring a Route-Based VPN Tunnel in a User Logical System on page 120

Example: Configuring IKE and IPsec SAs for a VPN Tunnel

The master administrator is responsible for assigning an st0 interface to a user logical system and configuring IKE and IPsec SAs at the root level for each VPN tunnel. This example shows how to assign an st0 interface to a user logical system and configure IKE and IPsec SA parameters.

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "“Understanding the Master Logical System and the Master Administrator Role” on page 8.
- Read Understanding Route-Based IPsec VPNs in the *Junos OS Security Configuration Guide*.

Overview

In this example you configure a VPN tunnel for the ls-product-design user logical system. This example configures the VPN tunnel parameters described in Table 17 on page 116.

Table 17: Logical System VPN Tunnel Configuration

Feature	Name	Configuration Parameters
Tunnel interface	st0 unit 1	Assigned to ls-product-design logical system
IKE proposal	ike-phase1-proposal	• Preshared keys authentication • Diffie-Hellman group 2 • sha1 authentication algorithm • aes-128-cbc encryption algorithm
IKE policy		• Main mode • References IKE proposal ike-phase1-proposal • ASCII preshared key 395psksecr3t

Table 17: Logical System VPN Tunnel Configuration *(continued)*

Feature	Name	Configuration Parameters
IKE gateway	ike-gw	• External interface ge-0/0/3.0 • References IKE policy ike-phase1-policy • Address 2.2.2.2
IPsec proposal	ipsec-phase2-proposal	• ESP protocol • hmac-sha1-96 authentication algorithm • aes-128-cbc encryption algorithm
IPsec policy	vpn-policy1	• References ipsec-phase2-proposal • perfect-forward-secrecy keys group2
VPN	ike-vpn	• bind-interface st0.1 • References ike-gw gateway • References vpn-policy1 policy
VPN monitoring		For ike-vpn VPN: • source-interface st0.1 • destination-ip 4.0.0.1

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 logical-systems ls-product-design interfaces st0 unit 1
set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy mode main
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text
   "$9$b92JGP5Q/ApmfIclv7NHqmfT39CuBRSAt87"
set security ike gateway ike-gw ike-policy ike-phase1-policy
set security ike gateway ike-gw address 2.2.2.2
set security ike gateway ike-gw external-interface ge-0/0/3.0
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group2
set security ipsec policy vpn-policy1 proposals ipsec-phase2-proposal
set security ipsec vpn ike-vpn bind-interface st0.1
set security ipsec vpn ike-vpn vpn-monitor source-interface st0.1
set security ipsec vpn ike-vpn vpn-monitor destination-ip 4.0.0.1
set security ipsec vpn ike-vpn ike gateway ike-gw
set security ipsec vpn ike-vpn ike ipsec-policy vpn-policy1
```

Step-by-Step Procedure

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

To assign a VPN tunnel interface to a user logical system and configure IKE and IPsec SAs:

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

```
[edit]
admin@host> configure
admin@host#
```

2. Assign a VPN tunnel interface.

```
[edit logical-systems ls-product-design]
admin@host# set interfaces st0 unit 1
```

3. Configure an IKE proposal.

```
[edit security ike]
admin@host# set proposal ike-phase1-proposal authentication-method
  pre-shared-keys
admin@host# set proposal ike-phase1-proposal dh-group group2
admin@host# set proposal ike-phase1-proposal authentication-algorithm sha1
admin@host# set proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
```

4. Configure an IKE policy.

```
[edit security ike]
admin@host# set policy ike-phase1-policy mode main
admin@host# set policy ike-phase1-policy proposals ike-phase1-proposal
admin@host# set policy ike-phase1-policy pre-shared-key ascii-text 395psksecr3t
```

5. Configure an IKE gateway.

```
[edit security ike]
admin@host# set gateway ike-gw external-interface ge-0/0/3.0
admin@host# set gateway ike-gw ike-policy ike-phase1-policy
admin@host# set gateway ike-gw address 2.2.2.2
```

6. Configure an IPsec proposal.

```
[edit security ipsec]
admin@host# set proposal ipsec-phase2-proposal protocol esp
admin@host# set proposal ipsec-phase2-proposal authentication-algorithm
  hmac-sha1-96
admin@host# set proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
```

7. Configure an IPsec policy.

```
[edit security ipsec]
admin@host# set policy vpn-policy1 proposals ipsec-phase2-proposal
admin@host# set policy vpn-policy1 perfect-forward-secrecy keys group2
```

8. Configure the VPN.

```
[edit security ipsec]
admin@host# set vpn ike-vpn bind-interface st0.1
admin@host# set vpn ike-vpn ike gateway ike-gw
```

```
admin@host# set vpn ike-vpn ike ipsec-policy vpn-policy1
```

9. Configure VPN monitoring.

```
[edit security ipsec]
admin@host# set vpn ike-vpn vpn-monitor source-interface st0.1
admin@host# set vpn ike-vpn vpn-monitor destination-ip 4.0.0.1
```

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

```
[edit]
admin@host# show interfaces
  st0 {
    unit 1;
  }
[edit]
admin@host# show security ike
  proposal ike-phase1-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
  }
    policy ike-phase1-policy {
      mode main;
      proposals ike-phase1-proposal;
      pre-shared-key ascii-text "$9$b92JGP5Q/ApmfIclv7NHqmfT39CuBRSAt87"; ##
        SECRET-DATA
    }
    gateway ike-gw {
      ike-policy ike-phase1-policy;
      address 2.2.2.2;
      external-interface ge-0/0/3.0;
    }
[edit]
admin@host# show security ipsec
  proposal ipsec-phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
  }
    policy vpn-policy1 {
      perfect-forward-secrecy {
        keys group2;
      }
      proposals ipsec-phase2-proposal;
    }
    vpn ike-vpn {
      bind-interface st0.1;
      vpn-monitor {
        source-interface st0.1;
        destination-ip 4.0.0.1;
      }
      ike {
```

```
        gateway ike-gw;
        ipsec-policy vpn-policy1;
    }
}
```

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

Verification

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose Verify that the IKE and IPsec SA configuration is correct.

Action From operational mode, enter the **show security ike** and **show security ipsec** commands.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring a Route-Based VPN Tunnel in a User Logical System on page 120
- Understanding Route-Based VPN Tunnels in Logical Systems on page 115
- User Logical System Configuration Overview on page 86

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

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 86.
- 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" on page 116.

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" on page 26.

You configure the route-based VPN parameters described in Table 18 on page 121.

Table 18: 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
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 in the *Junos OS CLI User Guide*.

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]
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.

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 123
- Verifying the IPsec Phase 2 Status on page 123

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 in the *Junos OS Security Configuration Guide*.

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 in the *Junos OS Security Configuration Guide*.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring a Route-Based VPN in the *Junos OS Security Configuration Guide*.
- Understanding Route-Based VPN Tunnels in Logical Systems on page 115
- User Logical System Configuration Overview on page 86

Understanding Logical System Network Address Translation

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 configured NAT

on a device that is not configured for logical systems. 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Network Address Translation for a User Logical System on page 124
- User Logical System Configuration Overview on page 86
- Understanding Logical Systems Security Profiles on page 34
- NAT Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Network Address Translation for a User Logical System

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

- Requirements on page 125
- Overview on page 125
- Configuration on page 125
- Verification on page 127

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical System Configuration Overview" on page 86.
- Use the **show system security-profile nat-static-rule** command to see the static NAT resources allocated to the logical system. See the *Junos OS CLI Reference*.
- Configure security policies. See "Example: Configuring Security Policies in a User Logical System" on page 104.

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" on page 26.

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 19 on page 125.

Table 19: 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
```

Step-by-Step Procedure

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

To configure 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;
            }
        }
```

```
}
```

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 127
- Verifying NAT Application to Traffic on page 127

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- User Logical System Configuration Overview on page 86
- Understanding Logical System Network Address Translation on page 123
- Static NAT Configuration Overview in the *Junos OS Security Configuration Guide*

IDP in Logical Systems Overview

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 on page 127
- IDP Installation and Licensing for Logical Systems on page 128

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding IDP Features in Logical Systems on page 129

- Example: Configuring an IDP Policy for a User Logical System on page 132
- Example: Configuring an IDP Policy for the Master Logical System on page 71
- User Logical System Configuration Overview on page 86
- Understanding Logical Systems Security Profiles on page 34
- IDP Policies Overview in the *Junos OS Security Configuration Guide*

Understanding IDP Features in Logical Systems

This topic includes the following sections:

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.

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, 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding IDP Policy Rulebases in the *Junos OS Security Configuration Guide*
- Understanding IDP Protocol Decoders in the *Junos OS Security Configuration Guide*
- IDP SSL Overview in the *Junos OS Security Configuration Guide*
- Understanding IDP Inline Tap Mode in the *Junos OS Security Configuration Guide*
- Understanding Multiple IDP Detector Support in the *Junos OS Security Configuration Guide*
- Understanding IDP Logging in the *Junos OS Security Configuration Guide*

Example: Configuring an IDP Policy for a User Logical System

The master administrator can *either* download predefined IDP policies to the device or configure custom IDP policies at the root level using custom or predefined attack objects. The master administrator is responsible for assigning an IDP policy to a user logical system. This example shows how to assign a predefined IDP policy to a user logical system.

Requirements

Before you begin:

- Log in to the master logical system as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.
- Read IDP Policies Overview in the *Junos OS Security Configuration Guide*.
- Assign the ls-design-profile security policy to the ls-product-design user logical system. See "Example: Configuring Logical Systems Security Profiles" on page 40.
- Download predefined IDP policy templates to the device. See Downloading and Using Predefined IDP Policy Templates (CLI Procedure) in the *Junos OS Security Configuration Guide*.

NOTE: **Activating a predefined IDP policy with the active-policy configuration statement at the [edit security idp] hierarchy level only applies to the master logical system. For a user logical system, the master administrator specifies the active IDP policy in the security profile that is bound to the user logical system.**

Overview

The predefined IDP policy named Recommended contains attack objects recommended by Juniper Networks. All rules in the policy have their actions set to take the recommended action for each attack object. You add the Recommended IDP policy to the ls-design-profile, which is bound to the ls-product-design user logical system shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26.

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 system security-profile ls-design-profile idp-policy Recommended
```

Step-by-Step Procedure

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

To add a predefined IDP policy to a security profile for a user logical system:

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

   ```
   [edit]
   admin@host> configure
   admin@host#
   ```

2. Add the IDP policy to the security profile.

   ```
   [edit system security-profile]
   admin@host# set ls-design-profile idp-policy Recommended
   ```

Results

From configuration mode, confirm your configuration by entering the **show security idp** and **show system security-profile ls-design-profile** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
admin@host# show security idp
  idp-policy Recommended {
    ...
  }
[edit]
admin@host# show system security-profile ls-design-profile
  policy {
    ...
  }
  idp-policy Recommended;
logical-system ls-product-design;
```

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

Verification

Verifying the Configuration

Purpose

Verify the IDP policy assigned to the logical system.

Action

From operational mode, enter the **show security idp logical-system policy-association** command. Ensure that the IDP policy in the security profile that is bound to the logical system is correct.

```
admin@host> show security idp logical-system policy-association
```

Logical system	IDP policy
ls-product-design	Recommended

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Enabling IDP in a User Logical System Security Policy on page 134
- IDP in Logical Systems Overview on page 127
- User Logical System Configuration Overview on page 86

Example: Enabling IDP in a User Logical System Security Policy

This example shows how to enable IDP in a security policy 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 86.
- Use the **show system security-profiles idp-policy** command to see the security policy resources allocated to the logical system. See the *Junos OS CLI Reference*.
- 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" on page 132.

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" on page 26.

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" on page 132.

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 in the *Junos OS CLI User Guide*.

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.

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

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring an IDP Policy for a User Logical System on page 132
- IDP in Logical Systems Overview on page 127
- User Logical System Configuration Overview on page 86

Understanding Logical System Application Identification Services

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 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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Junos OS Application Identification Services in the *Junos OS Security Configuration Guide*
- Example: Updating the Junos OS Application Identification Extracted Application Package Automatically in the *Junos OS Security Configuration Guide*
- Example: Configuring Junos OS Application Identification Custom Application Definitions in the *Junos OS Security Configuration Guide*
- Understanding IDP Application Identification in the *Junos OS Security Configuration Guide*
- Understanding the Application System Cache in the *Junos OS Security Configuration Guide*
- Verifying Application System Cache Statistics in the *Junos OS Security Configuration Guide*

Understanding Logical System Application Firewall Services

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 the *Junos OS Security Configuration Guide*.

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 on page 77
- Example: Configuring Application Firewall Services for a User Logical System on page 138

Example: Configuring Application Firewall Services for a User Logical System

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 the *Junos OS Security Configuration Guide*.

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 Systems Security Profiles" on page 34.
- 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 9.

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" on page 26.

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]
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 {
      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 141

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 86
- Understanding Logical System Application Firewall Services on page 137

Understanding Logical System Application Tracking Services

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding AppTrack in the *Junos OS Security Configuration Guide*
- Example: Configuring AppTrack in the *Junos OS Security Configuration Guide*
- Example: Configuring AppTrack for a User Logical System on page 143

Example: Configuring AppTrack for a User Logical System

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 86.
- (Master administrator) Configure system logging in the master logical system. See the *Junos OS 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" on page 26.

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]
   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 144
- Verifying Security Flow Session Statistics on page 144
- Verifying Application System Cache Statistics on page 145
- Verifying the Status of Application Identification Counter Values on page 145

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.

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Application Tracking Services on page 142
- User Logical System Configuration Overview on page 86
- Example: Verifying AppTrack Operation (CLI) in the *Junos OS Security Configuration Guide*

Example: Configuring User Logical Systems

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 86.
- 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 8.

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" on page 26.

This example configures the parameters described in Table 20 on page 146 and Table 21 on page 147.

Table 20: 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

Table 21: 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 148
- Configuring the ls-accounting-dept User Logical System on page 151

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 in the *Junos OS CLI User Guide*.

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.

```
[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
```

```
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;
      }
```



```
    }
  }
    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
```

```
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 in the *Junos OS CLI User Guide*.

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
```

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]
```

```
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;
        }
```

```
            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 155

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- User Logical System Configuration Overview on page 86
- Understanding Logical System Interfaces and Routing Instances on page 88
- Understanding Logical System Zones on page 95
- Understanding Logical System Security Policies on page 102

CHAPTER 4

Chassis Cluster Configuration

Understanding Logical Systems in the Context of Chassis Cluster

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring Logical Systems in an Active/Passive Chassis Cluster on page 158
- Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) on page 191
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 10
- Understanding Logical Systems for SRX Series Services Gateways on page 3
- Chassis Cluster Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster

This example shows how to configure logical systems in a basic active/passive chassis cluster.

NOTE: The master administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the master administrator or the user logical system administrator configures a user logical system. The configuration is synchronized between nodes in the cluster.

Requirements

Before you begin:

- Obtain two high-end SRX Series Services Gateways with identical hardware configurations. See Example: Configuring an SRX Series Services Gateway for the High-End as a Chassis Cluster in the *Junos OS Security Configuration Guide*. This chassis cluster deployment scenario includes the configuration of the SRX Series device for connections to an MX240 edge router and an EX8208 Ethernet Switch.
- Physically connect the two devices (back-to-back for the fabric and control ports) and ensure that they are the same models. You can configure both the fabric and control ports on the SRX5000 line. For the SRX1400 devices and the SRX3000 line, you can configure the fabric ports only. See Connecting SRX Series Hardware to Create a Chassis Cluster in the *Junos OS Security Configuration Guide*.
- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See Example: Setting the Chassis Cluster Node ID and Cluster ID in the *Junos OS Security Configuration Guide*.

NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the master administrator. Log in to the device as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.

NOTE: When you use SRX Series devices running logical systems in a chassis cluster, you must purchase and install the same number of logical system licenses for each node in the chassis cluster. Logical system licenses pertain to a single chassis or node within a chassis cluster and not to the cluster collectively. See "Understanding Licenses for Logical Systems on SRX Series Devices" on page 7.

Overview

In this example, the basic active/passive chassis cluster consists of two devices:

- One device actively provides logical systems, along with maintaining control of the chassis cluster.
- The other device passively maintains its state for cluster failover capabilities should the active device become inactive.

NOTE: Logical systems in an active/active chassis cluster are configured in a similar manner as for logical systems in an active/passive chassis cluster. For active/active chassis clusters, there can be multiple redundancy groups that can be primary on different nodes.

The master administrator configures the following logical systems on the primary device (node 0):

- Master logical system—The master administrator configures a security profile to provision portions of the system's security resources to the master logical system and configures the resources of the master logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The master administrator also configures security profiles to provision portions of the system's security resources to user logical systems. The user logical system administrator can then configure interfaces, routing, and security resources allocated to his or her logical system.
- Interconnect logical system LSYS0 that connects logical systems on the device—The master administrator configures logical tunnel interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for the establishment of tunnels.

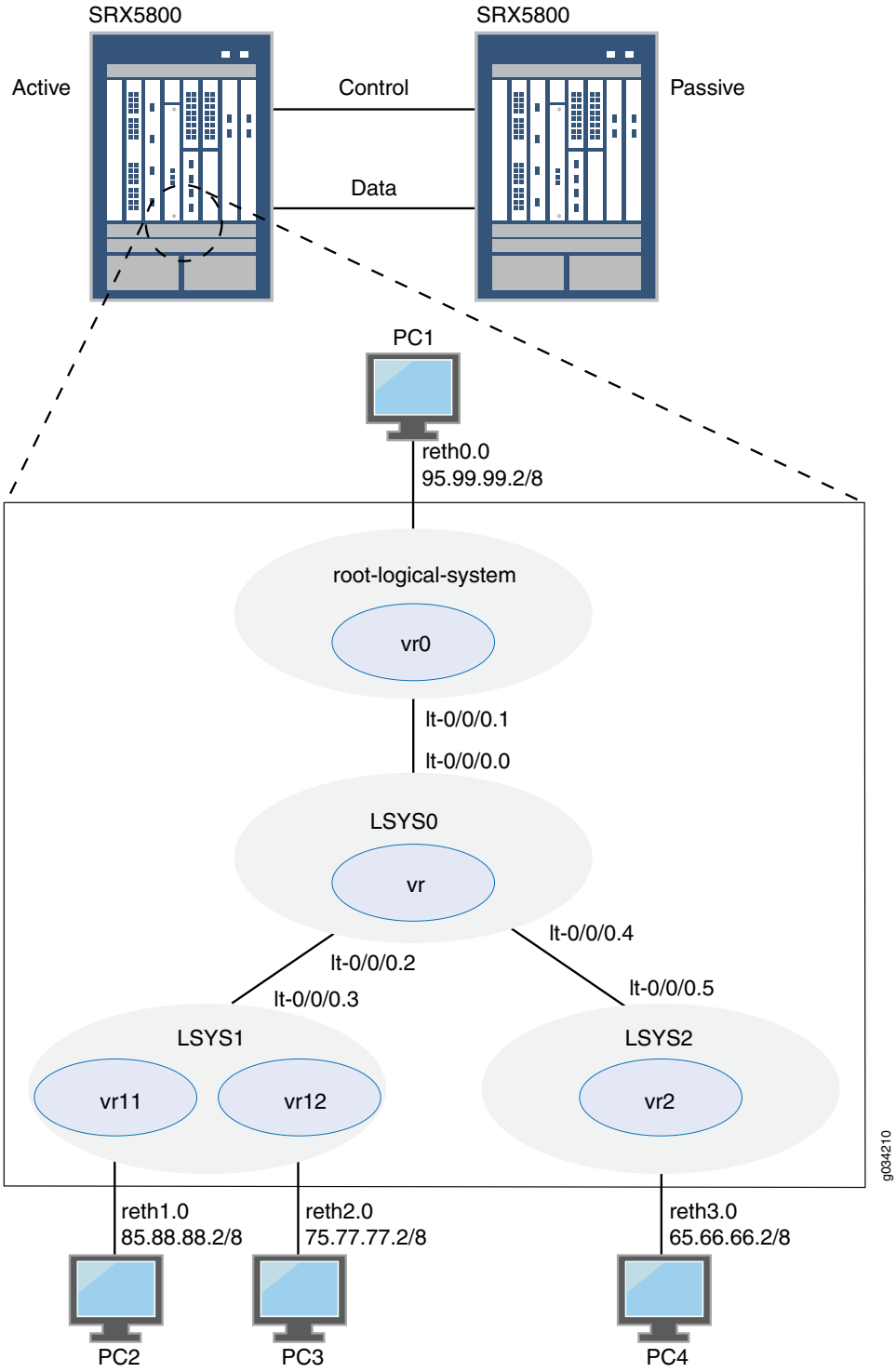
NOTE: This example does not describe configuring features such as NAT, IDP, or VPNs for a logical system. See "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 and "User Logical System Configuration Overview" on page 86 for more information about features that can be configured for logical systems.

If you are performing proxy ARP in a chassis cluster configuration, you must apply the proxy ARP configuration to the reth interfaces rather than the member interfaces because the reth interfaces contain the logical configurations. See Configuring Proxy ARP (CLI Procedure) in the *Junos OS Security Configuration Guide*.

Topology

Figure 5 on page 161 shows the topology used in this example.

Figure 5: Logical Systems in a Chassis Cluster



Configuration

Chassis Cluster Configuration (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, 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.

On {primary:node0}

```
set chassis cluster control-ports fpc 0 port 0
set chassis cluster control-ports fpc 6 port 0
set interfaces fab0 fabric-options member-interfaces ge-1/1/0
set interfaces fab1 fabric-options member-interfaces ge-7/1/0
set groups node0 system host-name SRX5800-1
set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
set groups node1 system host-name SRX5800-2
set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
set apply-groups “${node}”
set chassis cluster reth-count 5
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 100
set interfaces ge-1/0/0 gigether-options redundant-parent reth0
set interfaces ge-1/0/1 gigether-options redundant-parent reth1
set interfaces ge-1/0/2 gigether-options redundant-parent reth2
set interfaces ge-1/0/3 gigether-options redundant-parent reth3
set interfaces ge-7/0/0 gigether-options redundant-parent reth0
set interfaces ge-7/0/1 gigether-options redundant-parent reth1
set interfaces ge-7/0/2 gigether-options redundant-parent reth2
set interfaces ge-7/0/3 gigether-options redundant-parent reth3
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 95.99.99.1/8
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth3 redundant-ether-options redundancy-group 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 in the *Junos OS CLI User Guide*.

To configure a chassis cluster:

NOTE: Perform the following steps on the primary device (node 0). They are automatically copied over to the secondary device (node 1) when you execute a commit command.

1. Configure control ports for the clusters.

```
[edit chass cluster]
user@host# set control-ports fpc 0 port 0
user@host# set control-ports fpc 6 port 0
```

2. Configure the fabric (data) ports of the cluster that are used to pass RTOs in active/passive mode.

```
[edit interfaces]
user@host# set fab0 fabric-options member-interfaces ge-1/1/0
user@host# set fab1 fabric-options member-interfaces ge-7/1/0
```

3. Assign some elements of the configuration to a specific member. Configure out-of-band management on the fxp0 interface of the SRX Services Gateway using separate IP addresses for the individual control planes of the cluster.

```
[edit]
user@host# set groups node0 system host-name SRX5800-1
user@host# set groups node0 interfaces fxp0 unit 0 family inet address
  10.157.90.24/9
user@host# set groups node0 system backup-router 10.157.64.1 destination
  0.0.0.0/0
user@host# set groups node1 system host-name SRX5800-2
user@host# set groups node1 interfaces fxp0 unit 0 family inet address
  10.157.90.23/19
user@host# set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set apply-groups “${node}”
```

4. Configure redundancy groups for chassis clustering.

```
[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 0 node 0 priority 200
user@host# set redundancy-group 0 node 1 priority 100
user@host# set redundancy-group 1 node 0 priority 200
user@host# set redundancy-group 1 node 1 priority 100
```

5. Configure the data interfaces on the platform so that in the event of a data plane failover, the other chassis cluster member can take over the connection seamlessly.

```
[edit interfaces]
user@host# set ge-1/0/0 gigether-options redundant-parent reth0
user@host# set ge-1/0/1 gigether-options redundant-parent reth1
user@host# set ge-1/0/2 gigether-options redundant-parent reth2
```

```
user@host# set ge-1/0/3 gigether-options redundant-parent reth3
user@host# set ge-7/0/0 gigether-options redundant-parent reth0
user@host# set ge-7/0/1 gigether-options redundant-parent reth1
user@host# set ge-7/0/2 gigether-options redundant-parent reth2
user@host# set ge-7/0/3 gigether-options redundant-parent reth3
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 95.99.99.1/8
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth3 redundant-ether-options redundancy-group 1
```

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

```
user@host> show configuration
version ;
groups {
    node0 {
        system {
            host-name SRX58001;
            backup-router 10.157.64.1 destination 0.0.0.0/0;

        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.157.90.24/9;
                    }
                }
            }
        }
    }
    node1 {
        system {
            host-name SRX58002;
            backup-router 10.157.64.1 destination 0.0.0.0/0;

        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.157.90.23/19;
                    }
                }
            }
        }
    }
}
apply-groups "${node}";
chassis {
    cluster {
        control-link-recovery;
        reth-count 5;
        control-ports {
            fpc 0 port 0;
            fpc 6 port 0;
```

```
        }
        redundancy-group 0 {
            node 0 priority 200;
            node 1 priority 100;
        }
        redundancy-group 1 {
            node 0 priority 200;
            node 1 priority 100;
        }
    }
}
interfaces {
    ge-1/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-1/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-1/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-1/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    ge-7/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-7/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-7/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-7/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    fab0 {
        fabric-options {
            member-interfaces {
                ge-1/1/0;
            }
        }
    }
    fab1 {
        fabric-options {
```

```
            member-interfaces {
                ge-7/1/0;
            }
        }
    }
    reth0 {
        redundant-ether-options {
            redundancy-group 1;
        }
        unit 0 {
            family inet {
                address 95.99.99.1/8;
            }
        }
    }
    reth1 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth2 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth3 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
}
```

Logical System Configuration (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, 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.

NOTE: You are prompted to enter and then reenter plain-text passwords.

On {primary:node0}

```
set logical-systems LSYS1
set logical-systems LSYS2
set logical-systems LSYS0
set system login class lsys1 logical-system LSYS1
set system login class lsys1 permissions all
set system login user lsys1admin full-name lsys1-admin
set system login user lsys1admin class lsys1
set user lsys1admin authentication plain-text-password
set system login class lsys2 logical-system LSYS2
set system login class lsys2 permissions all
set system login user lsys2admin full-name lsys2-admin
```

```
set system login user lsys2admin class lsys2
set system login user lsys2admin authentication plain-text-password
set system security-profile SP-root policy maximum 200
set system security-profile SP-root policy reserved 100
set system security-profile SP-root zone maximum 200
set system security-profile SP-root zone reserved 100
set system security-profile SP-root flow-session maximum 200
set system security-profile SP-root flow-session reserved 100
set system security-profile SP-root root-logical-system
set system security-profile SP0 logical-system LSYS0
set system security-profile SP1 policy maximum 100
set system security-profile SP1 policy reserved 50
set system security-profile SP1 zone maximum 100
set system security-profile SP1 zone reserved 50
set system security-profile SP1 flow-session maximum 100
set system security-profile SP1 flow-session reserved 50
set system security-profile SP1 logical-system LSYS1
set system security-profile SP2 policy maximum 100
set system security-profile SP2 policy reserved 50
set system security-profile SP2 zone maximum 100
set system security-profile SP2 zone reserved 50
set system security-profile SP2 flow-session maximum 100
set system security-profile SP2 flow-session reserved 50
set system security-profile SP2 logical-system LSYS2
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 2.1.1.1/24
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface reth0.0
set routing-instances vr0 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr0 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr0 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
set security zones security-zone root-trust host-inbound-traffic system-services all
set security zones security-zone root-trust host-inbound-traffic protocols all
set security zones security-zone root-trust interfaces reth0.0
set security zones security-zone root-untrust host-inbound-traffic system-services all
set security zones security-zone root-untrust host-inbound-traffic protocols all
set security zones security-zone root-untrust interfaces lt-0/0/0.1
set security policies from-zone root-trust to-zone root-untrust policy
  root-Trust_to_root-Untrust match source-address any
set security policies from-zone root-trust to-zone root-untrust policy
  root-Trust_to_root-Untrust match destination-address any
set security policies from-zone root-trust to-zone root-untrust policy
  root-Trust_to_root-Untrust match application any
set security policies from-zone root-trust to-zone root-untrust policy
  root-Trust_to_root-Untrust then permit
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match source-address any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match destination-address any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust match application any
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust then permit
```

```
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match source-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match destination-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match application any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust then permit
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match source-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match destination-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match application any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  then permit
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet address 2.1.1.3/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet address 2.1.1.5/24
```

Step-by-Step Procedure

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

To create logical systems and user logical system administrators and configure the master and interconnect logical systems:

1. Create the interconnect and user logical systems.

   ```
   [edit logical-systems]
   user@host# set LSYS0
   user@host# set LSYS1
   user@host# set LSYS2
   ```

2. Configure user logical system administrators.

   a. Configure the user logical system administrator for LSYS1.

      ```
      [edit system login]
      user@host# set class lsys1 logical-system LSYS1
      user@host# set class lsys1 permissions all
      user@host# set user lsys1admin full-name lsys1-admin
      user@host# set user lsys1admin class lsys1
      user@host# set user lsys1admin authentication plain-text-password
      ```

b. Configure the user logical system administrator for LSYS2.

```
[edit system login]
user@host# set class lsys2 logical-system LSYS2
user@host# set class lsys2 permissions all
user@host# set user lsys2admin full-name lsys2-admin
user@host# set user lsys2admin class lsys2
user@host# set user lsys2admin authentication plain-text-password
```

3. Configure security profiles and assign them to logical systems.

a. Configure a security profile and assign it to the root logical system.

```
[edit system security-profile]
user@host# set SP-root policy maximum 200
user@host# set SP-root policy reserved 100
user@host# set SP-root zone maximum 200
user@host# set SP-root zone reserved 100
user@host# set SP-root flow-session maximum 200
user@host# set SP-root flow-session reserved 100
user@host# set SP-root root-logical-system
```

b. Assign a dummy security profile containing no resources to the interconnect logical system LSYS0.

```
[edit system security-profile]
user@host# set SP0 logical-system LSYS0
```

c. Configure a security profile and assign it to LSYS1.

```
[edit system security-profile]
user@host# set SP1 policy maximum 100
user@host# set SP1 policy reserved 50
user@host# set SP1 zone maximum 100
user@host# set SP1 zone reserved 50
user@host# set SP1 flow-session maximum 100
user@host# set SP1 flow-session reserved 50
user@host# set SP1 logical-system LSYS1
```

d. Configure a security profile and assign it to LSYS2.

```
[edit system security-profile]
user@host# set SP2 policy maximum 100
user@host# set SP2 policy reserved 50
user@host# set SP2 zone maximum 100
user@host# set SP2 zone reserved 50
user@host# set SP2 flow-session maximum 100
user@host# set SP2 flow-session reserved 50
user@host# set SP2 logical-system LSYS2
```

4. Configure the master logical system.

a. Configure logical tunnel interfaces.

```
[edit interfaces]
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 2.1.1.1/24
```

b. Configure a routing instance.

```
[edit routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface reth0.0
user@host# set vr0 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
user@host# set vr0 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
user@host# set vr0 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
```

c. Configure zones.

```
[edit security zones]
user@host# set security-zone root-trust host-inbound-traffic system-services
  all
user@host# set security-zone root-trust host-inbound-traffic protocols all
user@host# set security-zone root-trust interfaces reth0.0
user@host# set security-zone root-untrust host-inbound-traffic system-services
  all
user@host# set security-zone root-untrust host-inbound-traffic protocols all
user@host# set security-zone root-untrust interfaces lt-0/0/0.1
```

d. Configure security policies.

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

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

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

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

5. Configure the interconnect logical system.

a. Configure logical tunnel interfaces.

```
[edit logical-systems LSYS0 interfaces]
user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 0 peer-unit 1
user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
```

```
user@host# set lt-0/0/0 unit 2 peer-unit 3
user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
user@host# set lt-0/0/0 unit 4 peer-unit 5
```

b. Configure the VPLS routing instance.

```
[edit logical-systems LSYS0 routing-instances]
user@host# set vr instance-type vpls
user@host# set vr interface lt-0/0/0.0
user@host# set vr interface lt-0/0/0.2
user@host# set vr interface lt-0/0/0.4
```

6. Configure logical tunnel interfaces for the user logical systems.

a. Configure logical tunnel interfaces for LSYS1.

```
[edit logical-systems LSYS1 interfaces ]
user@host# set lt-0/0/0 unit 3 encapsulation ethernet
user@host# set lt-0/0/0 unit 3 peer-unit 2
user@host# set lt-0/0/0 unit 3 family inet address 2.1.1.3/24
```

b. Configure logical tunnel interfaces for LSYS2.

```
[edit logical-systems LSYS2 interfaces ]
user@host# set lt-0/0/0 unit 5 encapsulation ethernet
user@host# set lt-0/0/0 unit 5 peer-unit 4
user@host# set lt-0/0/0 unit 5 family inet address 2.1.1.5/24
```

Results From configuration mode, confirm the configuration for LSYS0 by entering the **show logical-systems LSYS0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
    unit 4 {
      encapsulation ethernet-vpls;
      peer-unit 5;
    }
  }
}
  routing-instances {
    vr {
      instance-type vpls;
      interface lt-0/0/0.0;
      interface lt-0/0/0.2;
      interface lt-0/0/0.4;
```

```
    }
  }
```

From configuration mode, confirm the configuration for the master logical system by entering the **show interfaces**, **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.

```
[edit]
user@host# show interfaces
lt-0/0/0 {
  unit 1 {
    encapsulation ethernet;
    peer-unit 0;
    family inet {
      address 2.1.1.1/24;
    }
  }
}
  ge-1/0/0 {
    gigether-options {
      redundant-parent reth0;
    }
  }
  ge-1/0/1 {
    gigether-options {
      redundant-parent reth1;
    }
  }
  ge-1/0/2 {
    gigether-options {
      redundant-parent reth2;
    }
  }
  ge-1/0/3 {
    gigether-options {
      redundant-parent reth3;
    }
  }
  ge-7/0/0 {
    gigether-options {
      redundant-parent reth0;
    }
  }
  ge-7/0/1 {
    gigether-options {
      redundant-parent reth1;
    }
  }
  ge-7/0/2 {
    gigether-options {
      redundant-parent reth2;
    }
  }
  ge-7/0/3 {
    gigether-options {
```

```
        redundant-parent reth3;
      }
    }
    fab0 {
      fabric-options {
        member-interfaces {
          ge-1/1/0;
        }
      }
    }
    fab1 {
      fabric-options {
        member-interfaces {
          ge-7/1/0;
        }
      }
    }
    reth0 {
      redundant-ether-options {
        redundancy-group 1;
      }
      unit 0 {
        family inet {
          address 95.99.99.1/8;
        }
      }
    }
    reth1 {
      redundant-ether-options {
        redundancy-group 1;
      }
    }
    reth2 {
      redundant-ether-options {
        redundancy-group 1;
      }
    }
    reth3 {
      redundant-ether-options {
        redundancy-group 1;
      }
    }
[edit]
user@host# show routing-instances
vr0 {
    instance-type virtual-router;
    interface lt-0/0/0.1;
    interface reth0.0;
    routing-options {
      static {
        route 85.0.0.0/8 next-hop 2.1.1.3;
        route 75.0.0.0/8 next-hop 2.1.1.3;
        route 65.0.0.0/8 next-hop 2.1.1.5;
      }
    }
}
```

```
[edit]
user@host# show security
policies {
    from-zone root-trust to-zone root-untrust {
        policy root-Trust_to_root-Untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-untrust to-zone root-trust {
        policy root-Untrust_to_root-Trust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-untrust to-zone root-untrust {
        policy root-Untrust_to_root-Untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-trust to-zone root-trust {
        policy root-Trust_to_root-Trust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
    zones {
        security-zone root-trust {
            host-inbound-traffic {
                system-services {
```

```
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          reth0.0;
        }
      }
      security-zone root-untrust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          lt-0/0/0.1;
        }
      }
    }
```

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

User Logical System Configuration (User Logical System Administrator)

CLI Quick Configuration

To quickly configure user logical systems, 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.

Enter the following commands while logged in as the user logical system administrator for LSYS1:

```
set interfaces reth1 unit 0 family inet address 85.88.88.1/8
set interfaces reth2 unit 0 family inet address 75.77.77.1/8
set routing-instances vr11 instance-type virtual-router
set routing-instances vr11 interface lt-0/0/0.3
set routing-instances vr11 interface reth1.0
set routing-instances vr11 routing-options static route 65.0.0.0/8 next-hop 2.1.1.5
set routing-instances vr11 routing-options static route 95.0.0.0/8 next-hop 2.1.1.1
set routing-instances vr12 instance-type virtual-router
set routing-instances vr12 interface reth2.0
set routing-instances vr12 routing-options interface-routes rib-group inet vr11vr12v4
set routing-instances vr12 routing-options static route 85.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 95.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 65.0.0.0/8 next-table vr11.inet.0
set routing-instances vr12 routing-options static route 2.1.1.0/24 next-table vr11.inet.0
set routing-options rib-groups vr11vr12v4 import-rib vr11.inet.0
set routing-options rib-groups vr11vr12v4 import-rib vr12.inet.0
set security zones security-zone lsys1-trust host-inbound-traffic system-services all
set security zones security-zone lsys1-trust host-inbound-traffic protocols all
```

```
set security zones security-zone lsys1-trust interfaces reth1.0
set security zones security-zone lsys1-trust interfaces lt-0/0/0.3
set security zones security-zone lsys1-untrust host-inbound-traffic system-services all
set security zones security-zone lsys1-untrust host-inbound-traffic protocols all
set security zones security-zone lsys1-untrust interfaces reth2.0
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match application any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust then permit
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match application any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  then permit
```

Enter the following commands while logged in as the user logical system administrator for LSYS2:

```
set interfaces reth3 unit 0 family inet address 65.66.66.1/8
set routing-instances vr2 instance-type virtual-router
set routing-instances vr2 interface lt-0/0/0.5
set routing-instances vr2 interface reth3.0
set routing-instances vr2 routing-options static route 75.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr2 routing-options static route 85.0.0.0/8 next-hop 2.1.1.3
set routing-instances vr2 routing-options static route 95.0.0.0/8 next-hop 2.1.1.1
set security zones security-zone lsys2-trust host-inbound-traffic system-services all
set security zones security-zone lsys2-trust host-inbound-traffic protocols all
set security zones security-zone lsys2-trust interfaces reth3.0
set security zones security-zone lsys2-untrust host-inbound-traffic system-services all
set security zones security-zone lsys2-untrust host-inbound-traffic protocols all
set security zones security-zone lsys2-untrust interfaces lt-0/0/0.5
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match source-address any
```

```
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match application any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust then permit
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match application any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust then permit
```

Step-by-Step Procedure

NOTE: The user logical system administrator performs the following configuration while logged into his or her user logical system. The master administrator can also configure a user logical system at the [edit logical-systems *logical-system*] hierarchy level.

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

To configure the LSYS1 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys1-admin@host:LSYS1# set reth1 unit 0 family inet address 85.88.88.1/8
lsys1-admin@host:LSYS1# set reth2 unit 0 family inet address 75.77.77.1/8
```

2. Configure routing.

```
[edit routing-instances]
lsys1-admin@host:LSYS1# set vr11 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr11 interface lt-0/0/0.3
```

```
lsys1-admin@host:LSYS1# set vr11 interface reth1.0
lsys1-admin@host:LSYS1# set vr11 routing-options static route 65.0.0.0/8 next-hop
  2.1.1.5
lsys1-admin@host:LSYS1# set vr11 routing-options static route 95.0.0.0/8 next-hop
  2.1.1.1
lsys1-admin@host:LSYS1# set vr12 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr12 interface reth2.0
lsys1-admin@host:LSYS1# set vr12 routing-options interface-routes rib-group inet
  vr11vr12v4
lsys1-admin@host:LSYS1# set vr12 routing-options static route 85.0.0.0/8 next-table
  vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 95.0.0.0/8 next-table
  vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 65.0.0.0/8 next-table
  vr11.inet.0
lsys1-admin@host:LSYS1# set vr12 routing-options static route 2.1.1.0/24 next-table
  vr11.inet.0

[edit routing-options]
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v4 import-rib vr11.inet.0
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v4 import-rib vr12.inet.0
```

3. Configure zones and security policies.

```
[edit security zones]
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
  system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
  protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces reth1.0
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces lt-0/0/0.3
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
  system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
  protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust interfaces reth2.0

[edit security policies from-zone lsys1-trust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
  source-address any
```

```
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-trust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match application any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust then permit
```

Step-by-Step Procedure

To configure the LSYS2 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys2-admin@host:LSYS2# set reth3 unit 0 family inet address 65.66.66.1/8
```

2. Configure routing.

```
[edit routing-instances]
lsys2-admin@host:LSYS2# set vr2 instance-type virtual-router
lsys2-admin@host:LSYS2# set vr2 interface lt-0/0/0.5
lsys2-admin@host:LSYS2# set vr2 interface reth3.0
lsys2-admin@host:LSYS2# set vr2 routing-options static route 75.0.0.0/8 next-hop
  2.1.1.3
lsys2-admin@host:LSYS2# set vr2 routing-options static route 85.0.0.0/8 next-hop
  2.1.1.3
lsys2-admin@host:LSYS2# set vr2 routing-options static route 95.0.0.0/8 next-hop
  2.1.1.1
```

3. Configure zones and security policies.

```
[edit security zones]
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
  system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
  protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust interfaces reth3.0
lsys2-admin@host:LSYS2# set security zones security-zone lsys2-untrust
  host-inbound-traffic system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust host-inbound-traffic
  protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust interfaces lt-0/0/0.5

[edit security policies from-zone lsys2-trust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust then permit

[edit security policies from-zone from-zone lsys2-untrust to-zone lsys2-trust]
```

```
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust then permit

[edit security policies from-zone lsys2-untrust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust then permit

[edit security policies from-zone lsys2-trust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match source-address
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust then permit
```

Results From configuration mode, confirm the configuration for LSYS1 by entering the **show interfaces**, **show routing-instances**, **show routing-options**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
lsys1-admin@host:LSYS1# show interfaces
interfaces {
    lt-0/0/0 {
        unit 3 {
            encapsulation ethernet;
            peer-unit 2;
            family inet {
                address 2.1.1.3/24;
            }
        }
    }
    reth1 {
        unit 0 {
            family inet {
                address 85.88.88.1/8;
            }
        }
    }
    reth2 {
        unit 0 {
            family inet {
                address 75.77.77.1/8;
            }
        }
```

```
    }
}
[edit]
lsys1-admin@host:LSYS1# show routing-instances
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.3;
        interface reth1.0;
        routing-options {
            static {
                route 65.0.0.0/8 next-hop 2.1.1.5;
                route 95.0.0.0/8 next-hop 2.1.1.1;
            }
        }
    }
    vr12 {
        instance-type virtual-router;
        interface reth2.0;
        routing-options {
            interface-routes {
                rib-group inet vr11vr12v4;
            }
            static {
                route 85.0.0.0/8 next-table vr11.inet.0;
                route 95.0.0.0/8 next-table vr11.inet.0;
                route 65.0.0.0/8 next-table vr11.inet.0;
                route 2.1.1.0/24 next-table vr11.inet.0;
            }
        }
    }
}
[edit]
lsys1-admin@host:LSYS1# show routing-options
rib-groups {
    vr11vr12v4 {
        import-rib [ vr11.inet.0 vr12.inet.0 ];
    }
}
[edit]
lsys1-admin@host:LSYS1# show security
security {
    policies {
        from-zone lsys1-trust to-zone lsys1-untrust {
            policy lsys1trust-to-lsys1untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone lsys1-untrust to-zone lsys1-trust {
```

```
    policy lsys1untrust-to-lsys1trust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone lsys1-untrust to-zone lsys1-untrust {
    policy lsys1untrust-to-lsys1untrust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
      }
    }
  }
  from-zone lsys1-trust to-zone lsys1-trust {
    policy lsys1trust-to-lsys1trust {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit;
      }
    }
  }
}
zones {
  security-zone lsys1-trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      reth1.0;
      lt-0/0/0.3;
    }
  }
  security-zone lsys1-untrust {
    host-inbound-traffic {
      system-services {
        all;
      }
```

```
            protocols {
                all;
            }
        }
        interfaces {
            reth2.0;
        }
    }
  }
}
```

From configuration mode, confirm the configuration for LSYS2 by entering the **show interfaces**, **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.

```
lsys2-admin@host:LSYS2# show interfaces
[edit]
  interfaces {
  lt-0/0/0 {
    unit 5 {
      encapsulation ethernet;
      peer-unit 4;
      family inet {
        address 2.1.1.5/24;
      }
    }
  }
  reth3 {
    unit 0 {
      family inet {
        address 65.66.66.1/8;
      }
    }
  }
}
[edit]
lsys2-admin@host:LSYS2# show routing-instances
routing-instances {
  vr2 {
    instance-type virtual-router;
    interface lt-0/0/0.5;
    interface reth3.0;
    routing-options {
      static {
        route 75.0.0.0/8 next-hop 2.1.1.3;
        route 85.0.0.0/8 next-hop 2.1.1.3;
        route 95.0.0.0/8 next-hop 2.1.1.1;
      }
    }
  }
}
[edit]
lsys2-admin@host:LSYS2# show security
security {
  policies {
```

```
    from-zone lsys2-trust to-zone lsys2-untrust {
      policy lsys2trust-to-lsys2untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys2-untrust to-zone lsys2-trust {
      policy lsys2untrust-to-lsys2trust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys2-untrust to-zone lsys2-untrust {
      policy lsys2untrust-to-lsys2untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys2-trust to-zone lsys2-trust {
      policy lsys2trust-to-lsys2trust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
  }
  zones {
    security-zone lsys2-trust {
      host-inbound-traffic {
        system-services {
          all;
        }
        protocols {
```

```
            all;
          }
        }
        interfaces {
          reth3.0;
        }
      }
      security-zone lsys2-untrust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          lt-0/0/0.5;
        }
      }
    }
  }
```

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

Verification

Confirm that the configuration is working properly.

Verifying Chassis Cluster Status

Purpose Verify the chassis cluster status, failover status, and redundancy group information.

Action From operational mode, enter the **show chassis cluster status** command.

```
{primary:node0}
show chassis cluster status
Cluster ID: 1
Node                  Priority          Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   200         primary        no       no
    node1                   100         secondary      no       no

Redundancy group: 1 , Failover count: 1
```

```
node0                   200         primary         no       no
node1                   100         secondary       no       no
```

Troubleshooting Chassis Cluster with Logs

Purpose Use these logs to identify any chassis cluster issues. You should run these logs on both nodes.

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

```
user@host> show log jsrpd
user@host> show log chassisd
user@host> show log messages
user@host> show log dcd
user@host> show traceoptions
```

Verifying Logical System Licenses

Purpose Verify information about logical system licenses.

Action From operational mode, enter the **show system license status logical-system all** command.

```
{primary:node0}
user@host> show system license status logical-system all
node0:
--------------------------------------------------------------------------
Logical system license status:

logical system name                 license status
root-logical-system                 enabled
LSYS0                               enabled
LSYS1                               enabled
LSYS2                               enabled
```

Verifying Logical System License Usage

Purpose Verify information about logical system license usage.

NOTE: The actual number of licenses used is only displayed on the primary node.

Action From operational mode, enter the **show system license** command.

```
{primary:node0}
user@host> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  logical-system                        4           25           0    permanent

Licenses installed:
  License identifier: JUNOS305013
  License version: 2
  Valid for device: JN110B54BAGB
```

```
  Features:
    logical-system-25 - Logical System Capacity
      permanent
```

Verifying Intra-Logical System Traffic on a Logical System

Purpose Verify information about currently active security sessions within a logical system.

Action From operational mode, enter the **show security flow session logical-system LSYS1** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000114, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1782, Valid
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 33, Bytes: 1881

  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 28, Bytes: 2329
Total sessions: 1

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000001, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14388, Valid
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

Verifying Intra-Logical System Traffic Within All Logical Systems

Purpose Verify information about currently active security sessions on all logical systems.

Action From operational mode, enter the **show security flow session logical-system all** command.

```
{primary:node0}
user@host> show security flow session logical-system all
node0:
--------------------------------------------------------------------------
```

```
Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000114, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1776, Valid
Logical system: LSYS1
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 33, Bytes: 1881

  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 28, Bytes: 2329
Total sessions: 1

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:

Session ID: 90000001, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14382, Valid
Logical system: LSYS1
  In: 85.88.88.2/34538 --> 75.77.77.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 75.77.77.2/23 --> 85.88.88.2/34538;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

Verifying Traffic Between User Logical Systems

Purpose Verify information about currently active security sessions between logical systems.

Action From operational mode, enter the **show security flow session logical-system *logical-system-name*** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1

node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000094, Policy name: root-Untrust_to_root-Trust/5, State: Active,
Timeout: 1768, Valid
  In: 75.77.77.2/34590 --> 95.99.99.2/23;tcp, If: lt-0/0/0.1, Pkts: 23, Bytes:
1351
  Out: 95.99.99.2/23 --> 75.77.77.2/34590;tcp, If: reth0.0, Pkts: 22, Bytes: 1880
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
```

```
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000002, Policy name: root-Untrust_to_root-Trust/5, State: Backup,
Timeout: 14384, Valid
  In: 75.77.77.2/34590 --> 95.99.99.2/23;tcp, If: lt-0/0/0.1, Pkts: 0, Bytes: 0
  Out: 95.99.99.2/23 --> 75.77.77.2/34590;tcp, If: reth0.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

{primary:node0}
user@host> show security flow session logical-system LSYS2

node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000089, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
 Timeout: 1790, Valid
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 40, Bytes:
2252
  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 32, Bytes: 2114
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000002, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
 Timeout: 14398, Valid
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

{primary:node0}
user@host> show security flow session logical-system all

node0:
```

```
---------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000088, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1782, Valid
Logical system: LSYS1
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: reth1.0, Pkts: 40, Bytes: 2252

  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: lt-0/0/0.3, Pkts: 32, Bytes:
2114

Session ID: 80000089, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
 Timeout: 1782, Valid
Logical system: LSYS2
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 40, Bytes:
2252
  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 32, Bytes: 2114
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
---------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000001, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14382, Valid
Logical system: LSYS1
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0

Session ID: 80000002, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
 Timeout: 14390, Valid
Logical system: LSYS2
  In: 85.88.88.2/34539 --> 65.66.66.2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
  Out: 65.66.66.2/23 --> 85.88.88.2/34539;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems in the Context of Chassis Cluster on page 157
- Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) on page 191
- Example: Configuring an SRX Series Services Gateway for the High-End as a Chassis Cluster in the *Junos OS Security Configuration Guide*

- Chassis Cluster Overview in the *Junos OS Security Configuration Guide*

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6)

This example shows how to configure logical systems in a basic active/passive chassis cluster with IPv6 addresses.

NOTE: The master administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the master administrator or the user logical system administrator configures a user logical system. The configuration is synchronized between nodes in the cluster.

Requirements

Before you begin:

- Obtain two high-end SRX Series Services Gateways with identical hardware configurations. See Example: Configuring an SRX Series Services Gateway for the High-End as a Chassis Cluster in the *Junos OS Security Configuration Guide*. This chassis cluster deployment scenario includes the configuration of the SRX Series device for connections to an MX240 edge router and an EX8208 Ethernet Switch.
- Physically connect the two devices (back-to-back for the fabric and control ports) and ensure that they are the same models. You can configure both the fabric and control ports on the SRX5000 line. For the SRX1400 devices and the SRX3000 line, you can configure the fabric ports only.
- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See Example: Setting the Chassis Cluster Node ID and Cluster ID in the *Junos OS Security Configuration Guide*.

NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the master administrator. Log in to the device as the master administrator. See "Understanding the Master Logical System and the Master Administrator Role" on page 8.

NOTE: When you use SRX Series devices running logical systems in a chassis cluster, you must purchase and install the same number of logical system licenses for each node in the chassis cluster. Logical system licenses pertain to a single chassis or node within a chassis cluster and not to the cluster collectively. See "Understanding Licenses for Logical Systems on SRX Series Devices" on page 7.

Overview

In this example, the basic active/passive chassis cluster consists of two devices:

- One device actively provides logical systems, along with maintaining control of the chassis cluster.
- The other device passively maintains its state for cluster failover capabilities should the active device become inactive.

NOTE: Logical systems in an active/active chassis cluster are configured in a similar manner as for logical systems in an active/passive chassis cluster. For active/active chassis clusters, there can be multiple redundancy groups that can be primary on different nodes.

The master administrator configures the following logical systems on the primary device (node 0):

- Master logical system—The master administrator configures a security profile to provision portions of the system's security resources to the master logical system and configures the resources of the master logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The master administrator also configures security profiles to provision portions of the system's security resources to user logical systems. The user logical system administrator can then configure interfaces, routing, and security resources allocated to his or her logical system.
- Interconnect logical system LSYS0 that connects logical systems on the device—The master administrator configures logical tunnel interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for the establishment of tunnels.

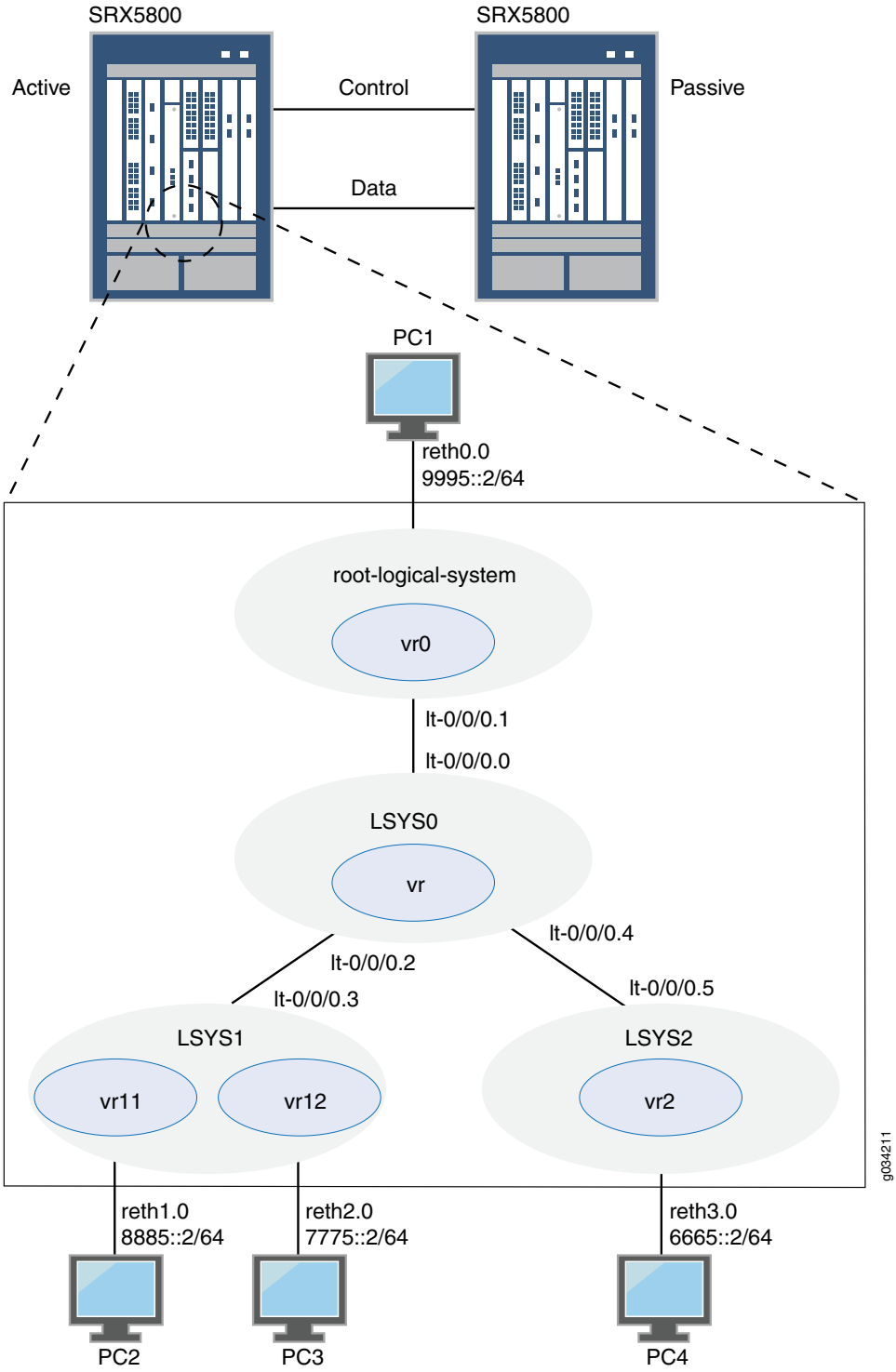
NOTE: This example does not describe configuring features such as NAT, IDP, or VPNs for a logical system. See "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 and "User Logical System Configuration Overview" on page 86 for more information about features that can be configured for logical systems.

If you are performing proxy ARP in a chassis cluster configuration, you must apply the proxy ARP configuration to the reth interfaces rather than the member interfaces because the reth interfaces contain the logical configurations. See Configuring Proxy ARP (CLI Procedure) in the *Junos OS Security Configuration Guide*.

Topology

Figure 6 on page 194 shows the topology used in this example.

Figure 6: Logical Systems in a Chassis Cluster (IPv6)



Configuration

Chassis Cluster Configuration with IPv6 Addresses (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, 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.

On {primary:node0}

```
set chassis cluster control-ports fpc 0 port 0
set chassis cluster control-ports fpc 6 port 0
set interfaces fab0 fabric-options member-interfaces ge-1/1/0
set interfaces fab1 fabric-options member-interfaces ge-7/1/0
set groups node0 system host-name SRX5800-1
set groups node0 interfaces fxp0 unit 0 family inet address 10.157.90.24/9
set groups node0 system backup-router 10.157.64.1 destination 0.0.0.0/0
set groups node1 system host-name SRX5800-2
set groups node1 interfaces fxp0 unit 0 family inet address 10.157.90.23/19
set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
set apply-groups “${node}”
set chassis cluster reth-count 5
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 100
set interfaces ge-1/0/0 gigether-options redundant-parent reth0
set interfaces ge-1/0/1 gigether-options redundant-parent reth1
set interfaces ge-1/0/2 gigether-options redundant-parent reth2
set interfaces ge-1/0/3 gigether-options redundant-parent reth3
set interfaces ge-7/0/0 gigether-options redundant-parent reth0
set interfaces ge-7/0/1 gigether-options redundant-parent reth1
set interfaces ge-7/0/2 gigether-options redundant-parent reth2
set interfaces ge-7/0/3 gigether-options redundant-parent reth3
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet6 address 9995::1/64
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth3 redundant-ether-options redundancy-group 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 in the *Junos OS CLI User Guide*.

To configure a chassis cluster:

NOTE: Perform the following steps on the primary device (node 0). They are automatically copied over to the secondary device (node 1) when you execute a commit command.

1. Configure control ports for the clusters.

```
[edit chassis cluster]
user@host# set control-ports fpc 0 port 0
user@host# set control-ports fpc 6 port 0
```

2. Configure the fabric (data) ports of the cluster that are used to pass RTOs in active/passive mode.

```
[edit interfaces]
user@host# set fab0 fabric-options member-interfaces ge-1/1/0
user@host# set fab1 fabric-options member-interfaces ge-7/1/0
```

3. Assign some elements of the configuration to a specific member. Configure out-of-band management on the fxp0 interface of the SRX Services Gateway using separate IP addresses for the individual control planes of the cluster.

```
[edit]
user@host# set groups node0 system host-name SRX5800-1
user@host# set groups node0 interfaces fxp0 unit 0 family inet address
  10.157.90.24/9
user@host# set groups node0 system backup-router 10.157.64.1 destination
  0.0.0.0/0
user@host# set groups node1 system host-name SRX5800-2
user@host# set groups node1 interfaces fxp0 unit 0 family inet address
  10.157.90.23/19
user@host# set groups node1 system backup-router 10.157.64.1 destination 0.0.0.0/0
user@host# set apply-groups “${node}”
```

4. Configure redundancy groups for chassis clustering.

```
[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 0 node 0 priority 200
user@host# set redundancy-group 0 node 1 priority 100
user@host# set redundancy-group 1 node 0 priority 200
user@host# set redundancy-group 1 node 1 priority 100
```

5. Configure the data interfaces on the platform so that in the event of a data plane failover, the other chassis cluster member can take over the connection seamlessly.

```
[edit interfaces]
user@host# set ge-1/0/0 gigether-options redundant-parent reth0
user@host# set ge-1/0/1 gigether-options redundant-parent reth1
user@host# set ge-1/0/2 gigether-options redundant-parent reth2
```

```
user@host# set ge-1/0/3 gigether-options redundant-parent reth3
user@host# set ge-7/0/0 gigether-options redundant-parent reth0
user@host# set ge-7/0/1 gigether-options redundant-parent reth1
user@host# set ge-7/0/2 gigether-options redundant-parent reth2
user@host# set ge-7/0/3 gigether-options redundant-parent reth3
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet6 address 9995::1/64
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth3 redundant-ether-options redundancy-group 1
```

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

```
user@host> show configuration
version ;
groups {
    node0 {
        system {
            host-name SRX58001;
            backup-router 10.157.64.1 destination 0.0.0.0/0;

        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.157.90.24/9;
                    }
                }
            }
        }
    }
    node1 {
        system {
            host-name SRX58002;
            backup-router 10.157.64.1 destination 0.0.0.0/0;

        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.157.90.23/19;
                    }
                }
            }
        }
    }
}
apply-groups "${node}";
chassis {
    cluster {
        control-link-recovery;
        reth-count 5;
        control-ports {
            fpc 0 port 0;
            fpc 6 port 0;
```

```
        }
        redundancy-group 0 {
            node 0 priority 200;
            node 1 priority 100;
        }
        redundancy-group 1 {
            node 0 priority 200;
            node 1 priority 100;
        }
    }
}
interfaces {
    ge-1/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-1/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-1/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-1/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    ge-7/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-7/0/1 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-7/0/2 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-7/0/3 {
        gigether-options {
            redundant-parent reth3;
        }
    }
    fab0 {
        fabric-options {
            member-interfaces {
                ge-1/1/0;
            }
        }
    }
    fab1 {
        fabric-options {
```

```
            member-interfaces {
                ge-7/1/0;
            }
        }
    }
    reth0 {
        redundant-ether-options {
            redundancy-group 1;
        }
        unit 0 {
            family inet6 {
                address 9995::1/64;
            }
        }
    }
    reth1 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth2 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
    reth3 {
        redundant-ether-options {
            redundancy-group 1;
        }
    }
}
```

Logical System Configuration with IPv6 Addresses (Master Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the master and interconnect logical systems, 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.

NOTE: You are prompted to enter and then reenter plain-text passwords.

On {primary:node0}

```
set logical-systems LSYS1
set logical-systems LSYS2
set logical-systems LSYS0
set system login class lsys1 logical-system LSYS1
set system login class lsys1 permissions all
set system login user lsys1admin full-name lsys1-admin
set system login user lsys1admin class lsys1
set user lsys1admin authentication plain-text-password
set system login class lsys2 logical-system LSYS2
set system login class lsys2 permissions all
set system login user lsys2admin full-name lsys2-admin
```

```
set system login user lsys2admin class lsys2
set system login user lsys2admin authentication plain-text-password
set system security-profile SP-root policy maximum 200
set system security-profile SP-root policy reserved 100
set system security-profile SP-root zone maximum 200
set system security-profile SP-root zone reserved 100
set system security-profile SP-root flow-session maximum 200
set system security-profile SP-root flow-session reserved 100
set system security-profile SP-root root-logical-system
set system security-profile SP0 logical-system LSYS0
set system security-profile SP1 policy maximum 100
set system security-profile SP1 policy reserved 50
set system security-profile SP1 zone maximum 100
set system security-profile SP1 zone reserved 50
set system security-profile SP1 flow-session maximum 100
set system security-profile SP1 flow-session reserved 50
set system security-profile SP1 logical-system LSYS1
set system security-profile SP2 policy maximum 100
set system security-profile SP2 policy reserved 50
set system security-profile SP2 zone maximum 100
set system security-profile SP2 zone reserved 50
set system security-profile SP2 flow-session maximum 100
set system security-profile SP2 flow-session reserved 50
set system security-profile SP2 logical-system LSYS2
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet6 address 2111::1/64
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface reth0.0
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 8885::/64 next-hop
    2111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 7775::/64 next-hop
    2111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 6665::/64 next-hop
    2111::5
set security zones security-zone root-trust host-inbound-traffic system-services all
set security zones security-zone root-trust host-inbound-traffic protocols all
set security zones security-zone root-trust interfaces reth0.0
set security zones security-zone root-untrust host-inbound-traffic system-services all
set security zones security-zone root-untrust host-inbound-traffic protocols all
set security zones security-zone root-untrust interfaces lt-0/0/0.1
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match source-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match destination-address any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust match application any
set security policies from-zone root-trust to-zone root-untrust policy
    root-Trust_to_root-Untrust then permit
set security policies from-zone root-untrust to-zone root-trust policy
    root-Untrust_to_root-Trust match source-address any
set security policies from-zone root-untrust to-zone root-trust policy
    root-Untrust_to_root-Trust match destination-address any
set security policies from-zone root-untrust to-zone root-trust policy
    root-Untrust_to_root-Trust match application any
```

```
set security policies from-zone root-untrust to-zone root-trust policy
  root-Untrust_to_root-Trust then permit
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match source-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match destination-address any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust match application any
set security policies from-zone root-untrust to-zone root-untrust policy
  root-Untrust_to_root-Untrust then permit
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match source-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match destination-address any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  match application any
set security policies from-zone root-trust to-zone root-trust policy root-Trust_to_root-Trust
  then permit
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet6 address 2111::3/64
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet6 address 2111::5/64
```

Step-by-Step Procedure

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

To create logical systems and user logical system administrators and configure the master and interconnect logical systems:

1. Create the interconnect and user logical systems.

   ```
   [edit logical-systems]
   user@host# set LSYS0
   user@host# set LSYS1
   user@host# set LSYS2
   ```

2. Configure user logical system administrators.

   a. Configure the user logical system administrator for LSYS1.

      ```
      [edit system login]
      user@host# set class lsys1 logical-system LSYS1
      user@host# set class lsys1 permissions all
      user@host# set user lsys1admin full-name lsys1-admin
      ```

```
user@host# set user lsys1admin class lsys1
user@host# set user lsys1admin authentication plain-text-password
```

b. Configure the user logical system administrator for LSYS2.

```
[edit system login]
user@host# set class lsys2 logical-system LSYS2
user@host# set class lsys2 permissions all
user@host# set user lsys2admin full-name lsys2-admin
user@host# set user lsys2admin class lsys2
user@host# set user lsys2admin authentication plain-text-password
```

3. Configure security profiles and assign them to logical systems.

a. Configure a security profile and assign it to the root logical system.

```
[edit system security-profile]
user@host# set SP-root policy maximum 200
user@host# set SP-root policy reserved 100
user@host# set SP-root zone maximum 200
user@host# set SP-root zone reserved 100
user@host# set SP-root flow-session maximum 200
user@host# set SP-root flow-session reserved 100
user@host# set SP-root root-logical-system
```

b. Assign a dummy security profile containing no resources to the interconnect logical system LSYS0.

```
[edit system security-profile]
user@host# set SP0 logical-system LSYS0
```

c. Configure a security profile and assign it to LSYS1.

```
[edit system security-profile]
user@host# set SP1 policy maximum 100
user@host# set SP1 policy reserved 50
user@host# set SP1 zone maximum 100
user@host# set SP1 zone reserved 50
user@host# set SP1 flow-session maximum 100
user@host# set SP1 flow-session reserved 50
user@host# set SP1 logical-system LSYS1
```

d. Configure a security profile and assign it to LSYS2.

```
[edit system security-profile]
user@host# set SP2 policy maximum 100
user@host# set SP2 policy reserved 50
user@host# set SP2 zone maximum 100
user@host# set SP2 zone reserved 50
user@host# set SP2 flow-session maximum 100
user@host# set SP2 flow-session reserved 50
user@host# set SP2 logical-system LSYS2
```

4. Configure the master logical system.

a. Configure logical tunnel interfaces.

```
[edit interfaces]
user@host# set lt-0/0/0 unit 1 encapsulation ethernet
```



```
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet6 address 2111::1/64
```

b. Configure a routing instance.

```
[edit routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface reth0.0
user@host# set vr0 routing-options rib vr0.inet6.0 static route 8885::/64
  next-hop 2111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 7775::/64 next-hop
  2111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 6665::/64
  next-hop 2111::5
```

c. Configure zones.

```
[edit security zones]
user@host# set security-zone root-trust host-inbound-traffic system-services
  all
user@host# set security-zone root-trust host-inbound-traffic protocols all
user@host# set security-zone root-trust interfaces reth0.0
user@host# set security-zone root-untrust host-inbound-traffic system-services
  all
user@host# set security-zone root-untrust host-inbound-traffic protocols all
user@host# set security-zone root-untrust interfaces lt-0/0/0.1
```

d. Configure security policies.

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

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

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

[edit security policies from-zone root-trust to-zone root-trust]
user@host# set policy root-Trust_to_root-Trust match source-address any
user@host# set policy root-Trust_to_root-Trust match destination-address any
user@host# set policy root-Trust_to_root-Trust match application any
```

```
user@host# set policy root-Trust_to_root-Trust then permit
```

5. Configure the interconnect logical system.

   a. Configure logical tunnel interfaces.

   ```
   [edit logical-systems LSYS0 interfaces]
   user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 0 peer-unit 1
   user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 2 peer-unit 3
   user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 4 peer-unit 5
   ```

   b. Configure the VPLS routing instance.

   ```
   [edit logical-systems LSYS0 routing-instances]
   user@host# set vr instance-type vpls
   user@host# set vr interface lt-0/0/0.0
   user@host# set vr interface lt-0/0/0.2
   user@host# set vr interface lt-0/0/0.4
   ```

6. Configure logical tunnel interfaces for the user logical systems.

   a. Configure logical tunnel interfaces for LSYS1.

   ```
   [edit logical-systems LSYS1 interfaces ]
   user@host# set lt-0/0/0 unit 3 encapsulation ethernet
   user@host# set lt-0/0/0 unit 3 peer-unit 2
   user@host# set lt-0/0/0 unit 3 family inet6 address 2111::3/64
   ```

   b. Configure logical tunnel interfaces for LSYS2.

   ```
   [edit logical-systems LSYS2 interfaces ]
   user@host# set lt-0/0/0 unit 5 encapsulation ethernet
   user@host# set lt-0/0/0 unit 5 peer-unit 4
   user@host# set lt-0/0/0 unit 5 family inet6 address 2111::5/64
   ```

Results From configuration mode, confirm the configuration for LSYS0 by entering the **show logical-systems LSYS0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
    }
    unit 4 {
      encapsulation ethernet-vpls;
      peer-unit 5;
```



```
    }
  }
}
  routing-instances {
    vr {
      instance-type vpls;
      interface lt-0/0/0.0;
      interface lt-0/0/0.2;
      interface lt-0/0/0.4;
    }
  }
```

From configuration mode, confirm the configuration for the master logical system by entering the **show interfaces**, **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.

```
[edit]
user@host# show interfaces
lt-0/0/0 {
  unit 1 {
    encapsulation ethernet;
    peer-unit 0;
    family inet6 {
      address 2111::1/64;
    }
  }
}
  ge-1/0/0 {
    gigether-options {
      redundant-parent reth0;
    }
  }
  ge-1/0/1 {
    gigether-options {
      redundant-parent reth1;
    }
  }
  ge-1/0/2 {
    gigether-options {
      redundant-parent reth2;
    }
  }
  ge-1/0/3 {
    gigether-options {
      redundant-parent reth3;
    }
  }
  ge-7/0/0 {
    gigether-options {
      redundant-parent reth0;
    }
  }
  ge-7/0/1 {
    gigether-options {
      redundant-parent reth1;
```

```
    }
  }
  ge-7/0/2 {
    gigether-options {
      redundant-parent reth2;
    }
  }
  ge-7/0/3 {
    gigether-options {
      redundant-parent reth3;
    }
  }
  fab0 {
    fabric-options {
      member-interfaces {
        ge-1/1/0;
      }
    }
  }
  fab1 {
    fabric-options {
      member-interfaces {
        ge-7/1/0;
      }
    }
  }
  reth0 {
    redundant-ether-options {
      redundancy-group 1;
    }
    unit 0 {
      family inet6 {
        address 9995::1/64;
      }
    }
  }
  reth1 {
    redundant-ether-options {
      redundancy-group 1;
    }
  }
  reth2 {
    redundant-ether-options {
      redundancy-group 1;
    }
  }
  reth3 {
    redundant-ether-options {
      redundancy-group 1;
    }
  }
[edit]
user@host# show routing-instances
vr0 {
  instance-type virtual-router;
  interface lt-0/0/0.1;
```

```
    interface reth0.0;
    routing-options {
        rib vr0.inet6.0 {
            static {
                route 8885::/64 next-hop 2111::3;
                route 7775::/64 next-hop 2111::3;
                route 6665::/64 next-hop 2111::5;
            }
        }
    }
}
[edit]
user@host# show security
policies {
    from-zone root-trust to-zone root-untrust {
        policy root-Trust_to_root-Untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-untrust to-zone root-trust {
        policy root-Untrust_to_root-Trust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-untrust to-zone root-untrust {
        policy root-Untrust_to_root-Untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone root-trust to-zone root-trust {
        policy root-Trust_to_root-Trust {
            match {
                source-address any;
                destination-address any;
                application any;
```

```
        }
        then {
          permit;
        }
      }
    }
  }
    zones {
      security-zone root-trust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          reth0.0;
        }
      }
      security-zone root-untrust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          lt-0/0/0.1;
        }
      }
    }
```

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

User Logical System Configuration with IPv6 (User Logical System Administrator)

CLI Quick Configuration

To quickly configure user logical systems, 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.

Enter the following commands while logged in as the user logical system administrator for LSYS1:

```
set interfaces reth1 unit 0 family inet6 address 8885::1/64
set interfaces reth2 unit 0 family inet6 address 7775::1/64
set routing-instances vr11 instance-type virtual-router
set routing-instances vr11 interface lt-0/0/0.3
set routing-instances vr11 interface reth1.0
set routing-instances vr11 routing-options rib vr11.inet6.0 static route 6665::/64 next-hop
  2111::5
```

```
set routing-instances vr11 routing-options rib vr11.inet6.0 static route 9995::/64 next-hop
  2111::1
set routing-instances vr12 instance-type virtual-router
set routing-instances vr12 interface reth2.0
set routing-instances vr12 routing-options interface-routes rib-group inet6 vr11vr12v6
set routing-instances vr12 rrouting-options rib vr12.inet6.0 static route 8885::/64
  next-table vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 9995::/64 next-table
  vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 6665::/64 next-table
  vr11.inet6.0
set routing-instances vr12 routing-options rib vr12.inet6.0 static route 2111::/64 next-table
  vr11.inet6.0
set routing-options rib-groups vr11vr12v6 import-rib vr11.inet6.0
set routing-options rib-groups vr11vr12v6 import-rib vr12.inet6.0
set security zones security-zone lsys1-trust host-inbound-traffic system-services all
set security zones security-zone lsys1-trust host-inbound-traffic protocols all
set security zones security-zone lsys1-trust interfaces reth1.0
set security zones security-zone lsys1-trust interfaces lt-0/0/0.3
set security zones security-zone lsys1-untrust host-inbound-traffic system-services all
set security zones security-zone lsys1-untrust host-inbound-traffic protocols all
set security zones security-zone lsys1-untrust interfaces reth2.0
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust match application any
set security policies from-zone lsys1-trust to-zone lsys1-untrust policy
  lsys1trust-to-lsys1untrust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-trust policy
  lsys1untrust-to-lsys1trust then permit
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match source-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match destination-address any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust match application any
set security policies from-zone lsys1-untrust to-zone lsys1-untrust policy
  lsys1untrust-to-lsys1untrust then permit
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match source-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match destination-address any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  match application any
set security policies from-zone lsys1-trust to-zone lsys1-trust policy lsys1trust-to-lsys1trust
  then permit
```

Enter the following commands while logged in as the user logical system administrator for LSYS2:

```
set interfaces reth3 unit 0 family inet6 address 6665::1/64
set routing-instances vr2 instance-type virtual-router
set routing-instances vr2 interface lt-0/0/0.5
set routing-instances vr2 interface reth3.0
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 7775::/64 next-hop
  2111::3
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 8885::/64 next-hop
  2111::3
set routing-instances vr2 routing-options rib vr2.inet6.0 static route 9995::/64 next-hop
  2111::1
set security zones security-zone lsys2-trust host-inbound-traffic system-services all
set security zones security-zone lsys2-trust host-inbound-traffic protocols all
set security zones security-zone lsys2-trust interfaces reth3.0
set security zones security-zone lsys2-untrust host-inbound-traffic system-services all
set security zones security-zone lsys2-untrust host-inbound-traffic protocols all
set security zones security-zone lsys2-untrust interfaces lt-0/0/0.5
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust match application any
set security policies from-zone lsys2-trust to-zone lsys2-untrust policy
  lsys2trust-to-lsys2untrust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-trust policy
  lsys2untrust-to-lsys2trust then permit
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match source-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match destination-address any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust match application any
set security policies from-zone lsys2-untrust to-zone lsys2-untrust policy
  lsys2untrust-to-lsys2untrust then permit
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match source-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match destination-address any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust match application any
set security policies from-zone lsys2-trust to-zone lsys2-trust policy
  lsys2trust-to-lsys2trust then permit
```

Step-by-Step Procedure

NOTE: The user logical system administrator performs the following configuration while logged into his or her user logical system. The master administrator can also configure a user logical system at the [edit logical-systems *logical-system*] hierarchy level.

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

To configure the LSYS1 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys1-admin@host:LSYS1# set reth1 unit 0 family inet6 address 8885::1/64
lsys1-admin@host:LSYS1# set reth2 unit 0 family inet6 address 7775::1/64
```

2. Configure routing.

```
[edit routing-instances]
lsys1-admin@host:LSYS1# set vr11 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr11 interface lt-0/0/0.3
lsys1-admin@host:LSYS1# set vr11 interface reth1.0
lsys1-admin@host:LSYS1# set vr11 routing-options rib vr11.inet6.0 static route
  6665::/64 next-hop 2111::5
lsys1-admin@host:LSYS1# set vr11 routing-options rib vr11.inet6.0 static route
  9995::/64 next-hop 2111::1
lsys1-admin@host:LSYS1# set vr12 instance-type virtual-router
lsys1-admin@host:LSYS1# set vr12 interface reth2.0
lsys1-admin@host:LSYS1# set vr12 routing-options interface-routes rib-group inet6
  vr11vr12v6
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
  8885::/64 next-table vr11.inet6.0
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
  9995::/64 next-table vr11.inet6.0
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
  6665::/64 next-table vr11.inet6.0
lsys1-admin@host:LSYS1# set vr12 routing-options rib vr12.inet6.0 static route
  2111::/64 next-table vr11.inet6.0

[edit routing-options]
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v6 import-rib vr11.inet6.0
lsys1-admin@host:LSYS1# set rib-groups vr11vr12v6 import-rib vr12.inet6.0
```

3. Configure zones and security policies.

```
[edit security zones]
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
  system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust host-inbound-traffic
  protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces reth1.0
lsys1-admin@host:LSYS1# set security-zone lsys1-trust interfaces lt-0/0/0.3
```

```
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
  system-services all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust host-inbound-traffic
  protocols all
lsys1-admin@host:LSYS1# set security-zone lsys1-untrust interfaces reth2.0

[edit security policies from-zone lsys1-trust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1trust then permit

[edit security policies from-zone lsys1-untrust to-zone lsys1-untrust]
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
  source-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust match application
  any
lsys1-admin@host:LSYS1# set policy lsys1untrust-to-lsys1untrust then permit

[edit security policies from-zone lsys1-trust to-zone lsys1-trust]
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match source-address
  any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match
  destination-address any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust match application any
lsys1-admin@host:LSYS1# set policy lsys1trust-to-lsys1trust then permit
```

Step-by-Step Procedure

To configure the LSYS2 user logical system:

1. Configure interfaces.

```
[edit interfaces]
lsys2-admin@host:LSYS2# set reth3 unit 0 family inet6 address 6665::1/64
```

2. Configure routing.

```
[edit routing-instances]
lsys2-admin@host:LSYS2# set vr2 instance-type virtual-router
lsys2-admin@host:LSYS2# set vr2 interface lt-0/0/0.5
lsys2-admin@host:LSYS2# set vr2 interface reth3.0
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
  7775::/64 next-hop 2111::3
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
  8885::/64 next-hop 2111::3
```

```
lsys2-admin@host:LSYS2# set vr2 routing-options rib vr2.inet6.0 static route
  9995::/64 next-hop 2111::1
```

3. Configure zones and security policies.

```
[edit security zones]
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
  system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust host-inbound-traffic
  protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-trust interfaces reth3.0
lsys2-admin@host:LSYS2# set security zones security-zone lsys2-untrust
  host-inbound-traffic system-services all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust host-inbound-traffic
  protocols all
lsys2-admin@host:LSYS2# set security-zone lsys2-untrust interfaces lt-0/0/0.5

[edit security policies from-zone lsys2-trust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2untrust then permit

[edit security policies from-zone from-zone lsys2-untrust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2trust then permit

[edit security policies from-zone lsys2-untrust to-zone lsys2-untrust]
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
  source-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2untrust-to-lsys2untrust then permit

[edit security policies from-zone lsys2-trust to-zone lsys2-trust]
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match source-address
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match
  destination-address any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust match application
  any
lsys2-admin@host:LSYS2# set policy lsys2trust-to-lsys2trust then permit
```

Results From configuration mode, confirm the configuration for LSYS1 by entering the **show interfaces**, **show routing-instances**, **show routing-options**, and **show security** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
lsys1-admin@host:LSYS1# show interfaces
interfaces {
    lt-0/0/0 {
        unit 3 {
            encapsulation ethernet;
            peer-unit 2;
            family inet6 {
                address 2111::3/64;
            }
        }
    }
    reth1 {
        unit 0 {
            family inet6 {
                address 8885::1/64;
            }
        }
    }
    reth2 {
        unit 0 {
            family inet6 {
                address 7775::1/64;
            }
        }
    }
}
[edit]
lsys1-admin@host:LSYS1# show routing-instances
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.3;
        interface reth1.0;
        routing-options {
            rib vr11.inet6.0 {
                static {
                    route 6665::/64 next-hop 2111::5;
                    route 9995::/64 next-hop 2111::1;
                }
            }
        }
    }
    vr12 {
        instance-type virtual-router;
        interface reth2.0;
        routing-options {
            interface-routes {
                rib-group inet6 vr11vr12v6;
            }
            rib vr12.inet6.0 {
                static {
                    route 8885::/64 next-table vr11.inet6.0;
                    route 9995::/64 next-table vr11.inet6.0;
                    route 6665::/64 next-table vr11.inet6.0;
                    route 2111::/64 next-table vr11.inet6.0;
```

```
        }
      }
    }
  }
}
[edit]
lsys1-admin@host:LSYS1# show routing-options
rib-groups {
  vr11vr12v6 {
    import-rib [ vr11.inet6.0 vr12.inet6.0 ];
  }
}
[edit]
lsys1-admin@host:LSYS1# show security
security {
  policies {
    from-zone lsys1-trust to-zone lsys1-untrust {
      policy lsys1trust-to-lsys1untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys1-untrust to-zone lsys1-trust {
      policy lsys1untrust-to-lsys1trust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys1-untrust to-zone lsys1-untrust {
      policy lsys1untrust-to-lsys1untrust {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone lsys1-trust to-zone lsys1-trust {
      policy lsys1trust-to-lsys1trust {
        match {
          source-address any;
```

```
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
    }
    zones {
      security-zone lsys1-trust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          reth1.0;
          lt-0/0/0.3;
        }
      }
      security-zone lsys1-untrust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          reth2.0;
        }
      }
    }
  }
```

From configuration mode, confirm the configuration for LSYS2 by entering the **show interfaces**, **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.

```
[edit]
lsys2-admin@host:LSYS2# show interfaces
interfaces {
  lt-0/0/0 {
    unit 5 {
      encapsulation ethernet;
      peer-unit 4;
      family inet6 {
        address 2111::5/64;
      }
    }
```

```
    }
    reth3 {
      unit 0 {
        family inet6 {
          address 6665::1/64;
        }
      }
    }
}
[edit]
lsys2-admin@host:LSYS2# show routing-instances
routing-instances {
    vr2 {
      instance-type virtual-router;
      interface lt-0/0/0.5;
      interface reth3.0;
      routing-options {
        rib vr2.inet6.0 {
          static {
            route 7775::/64 next-hop 2111::3;
            route 8885::/64 next-hop 2111::3;
            route 9995::/64 next-hop 2111::1;
          }
        }
      }
    }
}
[edit]
lsys2-admin@host:LSYS2# show security
security {
    policies {
      from-zone lsys2-trust to-zone lsys2-untrust {
        policy lsys2trust-to-lsys2untrust {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone lsys2-untrust to-zone lsys2-trust {
        policy lsys2untrust-to-lsys2trust {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone lsys2-untrust to-zone lsys2-untrust {
```

```
        policy lsys2untrust-to-lsys2untrust {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone lsys2-trust to-zone lsys2-trust {
        policy lsys2trust-to-lsys2trust {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
    }
    zones {
      security-zone lsys2-trust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          reth3.0;
        }
      }
      security-zone lsys2-untrust {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
        interfaces {
          lt-0/0/0.5;
        }
      }
    }
  }
```

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

Verification

Confirm that the configuration is working properly.

Verifying Chassis Cluster Status (IPv6)

Purpose Verify the chassis cluster status, failover status, and redundancy group information.

Action From operational mode, enter the **show chassis cluster status** command.

```
{primary:node0}
show chassis cluster status
Cluster ID: 1
Node                  Priority          Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   200         primary        no       no
    node1                   100         secondary      no       no

Redundancy group: 1 , Failover count: 1
    node0                   200         primary        no       no
    node1                   100         secondary      no       no
```

Troubleshooting Chassis Cluster with Logs (IPv6)

Purpose Use these logs to identify any chassis cluster issues. You should run these logs on both nodes.

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

```
user@host> show log jsrpd
user@host> show log chassisd
user@host> show log messages
user@host> show log dcd
user@host> show traceoptions
```

Verifying Logical System Licenses (IPv6)

Purpose Verify information about logical system licenses.

Action From operational mode, enter the **show system license status logical-system all** command.

```
{primary:node0}
user@host> show system license status logical-system all
```

```
node0:
--------------------------------------------------------------------------
Logical system license status:

logical system name                 license status
root-logical-system                 enabled
LSYS0                               enabled
LSYS1                               enabled
LSYS2                               enabled
```

Verifying Logical System License Usage (IPv6)

Purpose Verify information about logical system license usage.

NOTE: The actual number of licenses used is only displayed on the primary node.

Action From operational mode, enter the **show system license** command.

```
{primary:node0}
user@host> show system license
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  logical-system                        4           25           0    permanent

Licenses installed:
  License identifier: JUNOS305013
  License version: 2
  Valid for device: JN110B54BAGB
  Features:
    logical-system-25 - Logical System Capacity
      permanent
```

Verifying Intra-Logical System Traffic on a Logical System (IPv6)

Purpose Verify information about currently active security sessions within a logical system.

Action From operational mode, enter the **show security flow session logical-system LSYS1** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000115, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1784, Valid
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 22, Bytes: 1745
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 19, Bytes: 2108
Total sessions: 1

Flow Sessions on FPC2 PIC0:
```

```
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000006, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14392, Valid
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

Verifying Intra-Logical System Traffic Within All Logical Systems (IPv6)

Purpose Verify information about currently active security sessions on all logical systems.

Action From operational mode, enter the **show security flow session logical-system all** command.

```
{primary:node0}
user@host> show security flow session logical-system all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000115, Policy name: lsys1trust-to-lsys1untrust/8, State: Active,
Timeout: 1776, Valid
Logical system: LSYS1
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 22, Bytes: 1745
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 19, Bytes: 2108
Total sessions: 1

Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:

Session ID: 10000006, Policy name: lsys1trust-to-lsys1untrust/8, State: Backup,
Timeout: 14384, Valid
Logical system: LSYS1
  In: 8885::2/34564 --> 7775::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 7775::2/23 --> 8885::2/34564;tcp, If: reth2.0, Pkts: 0, Bytes: 0
Total sessions: 1
```

```
Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

Verifying Traffic Between User Logical Systems (IPv6)

Purpose Verify information about currently active security sessions between logical systems.

Action From operational mode, enter the **show security flow session logical-system *logical-system-name*** command.

```
{primary:node0}
user@host> show security flow session logical-system LSYS1

node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000118, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1792, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 65, Bytes: 6701
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000010, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14388, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

{primary:node0}
user@host> show security flow session logical-system LSYS2

node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000119, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
 Timeout: 1788, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 65, Bytes: 6701
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000011, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
 Timeout: 14380, Valid
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC2 PIC1:
Total sessions: 0

{primary:node0}
user@host> show security flow session logical-system all

node0:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 80000118, Policy name: lsys1trust-to-lsys1trust/11, State: Active,
Timeout: 1784, Valid
Logical system: LSYS1
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 65, Bytes: 6701

Session ID: 80000119, Policy name: lsys2untrust-to-lsys2trust/13, State: Active,
 Timeout: 1784, Valid
Logical system: LSYS2
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 91, Bytes: 6802
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 65, Bytes: 6701
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC0 PIC1:
Total sessions: 0

Flow Sessions on FPC2 PIC0:
```

```
Session ID: 80000010, Policy name: lsys1trust-to-lsys1trust/11, State: Backup,
Timeout: 14378, Valid
Logical system: LSYS1
  In: 8885::2/34565 --> 6665::2/23;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: lt-0/0/0.3, Pkts: 0, Bytes: 0

Session ID: 80000011, Policy name: lsys2untrust-to-lsys2trust/13, State: Backup,
 Timeout: 14376, Valid
Logical system: LSYS2
  In: 8885::2/34565 --> 6665::2/23;tcp, If: lt-0/0/0.5, Pkts: 0, Bytes: 0
  Out: 6665::2/23 --> 8885::2/34565;tcp, If: reth3.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC2 PIC1:
Total sessions: 0
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical Systems in the Context of Chassis Cluster on page 157
- Example: Configuring Logical Systems in an Active/Passive Chassis Cluster on page 158
- Example: Configuring an SRX Series Services Gateway for the High-End as a Chassis Cluster in the *Junos OS Security Configuration Guide*
- Chassis Cluster Overview in the *Junos OS Security Configuration Guide*

CHAPTER 5

IPv6 Configuration

IPv6 Addresses in Logical Systems Overview

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding IP Version 6 (IPv6) in the *Junos OS Security Configuration Guide*
- About IPv6 Address Types and How Junos OS for SRX Series Services Gateway and J-series Devices Use Them in the *Junos OS Security Configuration Guide*
- Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems on page 226
- Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) on page 191
- Understanding IPv6 Dual-Stack Lite in Logical Systems on page 241

Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems

This topic covers configuration of IPv6 interfaces, static routes, and routing instances for the master and interconnect logical systems. It also covers configuration of IPv6 logical tunnel interfaces for user logical systems.

Requirements

Before you begin:

- See "SRX Series Logical System Master Administrator Configuration Tasks Overview" on page 23 to understand how and where this procedure fits in the overall master administrator configuration process.
- See "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 26.
- See "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 10.

Overview

This scenario shows how to configure interfaces for the logical systems on the device, including an interconnect logical system.

- For the interconnect logical system, the example configures logical tunnel interfaces lt-0/0/0.0, lt-0/0/0.2, and lt-0/0/0.4. The example configures a routing instance called vr and assigns the interfaces to it.

  Because the interconnect logical system acts as a virtual switch, it is configured as a VPLS routing instance type. The interconnect logical system's lt-0/0/0 interfaces are configured with ethernet-vpls as the encapsulation type. The corresponding peer

lt-0/0/0 interfaces in the master and user logical systems are configured with Ethernet as the encapsulation type.

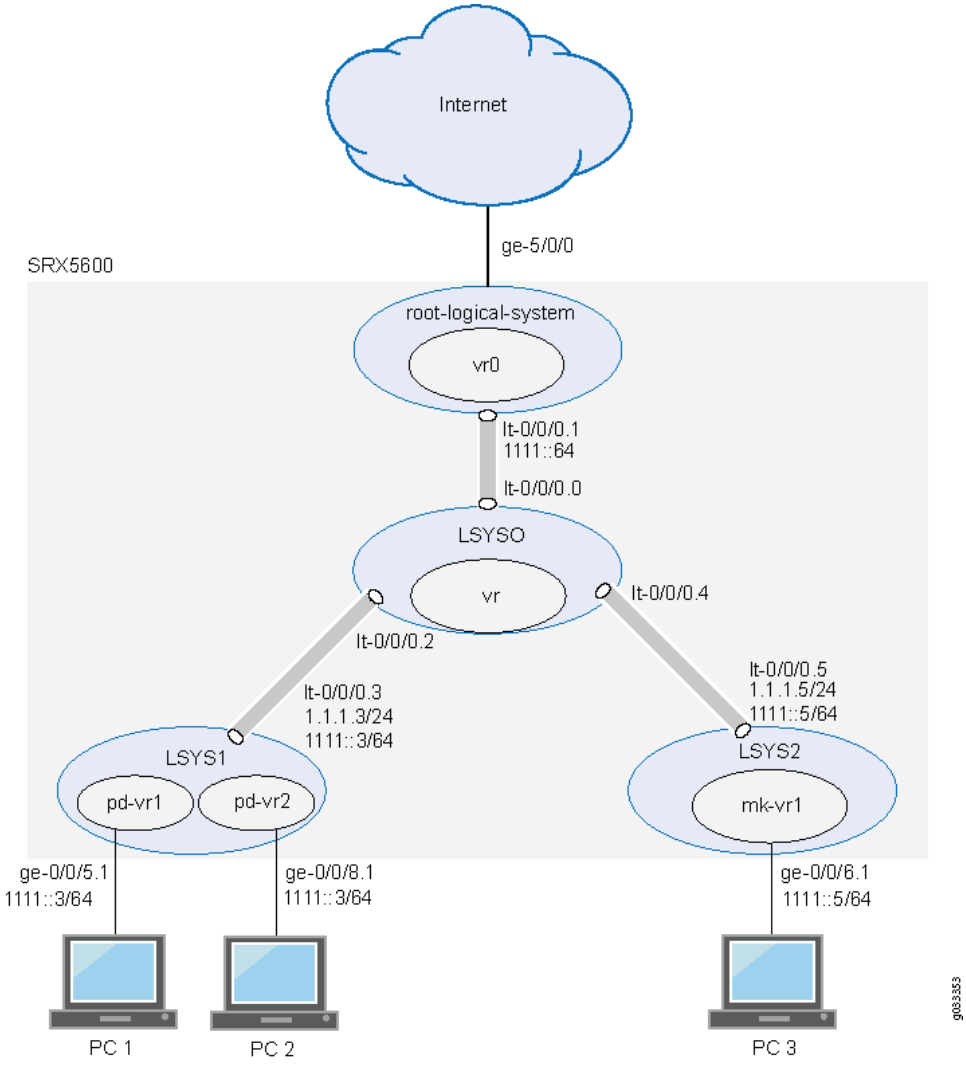
- lt-0/0/0.0 connects to lt-0/0/0.1 on the root logical system.
- lt-0/0/0.2 connects to lt-0/0/0.3 on the LSYS1 logical system.
- lt-0/0/0.4 connects to lt-0/0/0.5 on the LSYS2 logical system.

- For the master logical system, called root-logical-system, the example configures ge-5/0/0 and assigns it to the vr0 routing instance. The example configures lt-0/0/0.1 to connect to lt-0/0/0.0 on the interconnect logical system and assigns it to the vr0 routing instance. The example configures static routes to allow for communication with other logical systems and assigns them to the vr0 routing instance.
- For the LSYS1 logical system, the example configures lt-0/0/0.3 to connect to lt-0/0/0.2 on the interconnect logical system.
- For the LSYS2 logical system, the example configures lt-0/0/0.5 to connect to lt-0/0/0.4 on the interconnect logical system.

Figure 7 on page 228 shows the topology for this deployment including virtual routers and their interfaces for all IPv6 logical systems.

Topology

Figure 7: Configuring IPv6 Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers



Configuration

This topic explains how to configure interfaces for logical systems.

- Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System on page 229
- Configuring Interfaces, a Routing Instance, and Static Routes for the Master Logical System on page 230
- Configuring Logical Tunnel Interfaces for the User Logical Systems on page 232

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect 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 forwarding-options family inet6 mode flow-based
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 0 peer-unit 1
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 2 peer-unit 3
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 encapsulation ethernet-vpls
set logical-systems LSYS0 interfaces lt-0/0/0 unit 4 peer-unit 5
set logical-systems LSYS0 routing-instances vr instance-type vpls
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.0
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.2
set logical-systems LSYS0 routing-instances vr interface lt-0/0/0.4
```

Step-by-Step Procedure

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

To configure the interconnect system lt-0/0/0 interfaces and routing instances:

1. Enable flow-based forwarding for IPv6 traffic.

   ```
   [edit security]
   user@host# set forwarding-options family inet6 mode flow-based
   ```

2. Configure the lt-0/0/0 interfaces.

   ```
   [edit logical-systems LSYS0 interfaces]
   user@host# set lt-0/0/0 unit 0 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 0 peer-unit 1
   user@host# set lt-0/0/0 unit 2 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 2 peer-unit 3
   user@host# set lt-0/0/0 unit 4 encapsulation ethernet-vpls
   user@host# set lt-0/0/0 unit 4 peer-unit 5
   ```

3. Configure the routing instance for the interconnect logical system and add its lt-0/0/0 interfaces to it.

   ```
   [edit logical-systems LSYS0 routing-instances]
   user@host# set vr instance-type vpls
   user@host# set vr interface lt-0/0/0.0
   user@host# set vr interface lt-0/0/0.2
   user@host# set vr interface lt-0/0/0.4
   ```

Results

From configuration mode, confirm your configuration by entering the **show logical-systems interconnect-logical-system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

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

```
user@host# show logical-systems LSYS0
interfaces {
  lt-0/0/0 {
    unit 0 {
      encapsulation ethernet-vpls;
      peer-unit 1;
    }
    unit 2 {
      encapsulation ethernet-vpls;
      peer-unit 3;
      }
      unit 4 {
        encapsulation ethernet-vpls;
        peer-unit 5;
      }
    }
  }
    routing-instances {
      vr {
        instance-type vpls;
        interface lt-0/0/0.0;
        interface lt-0/0/0.2;
        interface lt-0/0/0.4;
      }
    }
```

Configuring Interfaces, a Routing Instance, and Static Routes for the Master 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-5/0/0 vlan-tagging
set interfaces ge-5/0/0 unit 0 vlan-id 600
set interfaces lt-0/0/0 unit 1 encapsulation Ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 0
set interfaces lt-0/0/0 unit 1 family inet address 1.1.1.1/24
set interfaces lt-0/0/0 unit 1 family inet6 address 1111::1/64
set interfaces ge-5/0/0 unit 0 family inet address 99.99.99.1/24
set interfaces ge-5/0/0 unit 0 family inet6 address 9999::1/64
set routing-instances vr0 instance-type virtual-router
set routing-instances vr0 interface lt-0/0/0.1
set routing-instances vr0 interface ge-5/0/0.0
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 7777::/64 next-hop
  1111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 8888::/64 next-hop
  1111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 6666::/64 next-hop
  1111::5
set routing-instances vr0 routing-options static route 77.77.77.0/24 next-hop 1.1.1.3
set routing-instances vr0 routing-options static route 88.88.88.0/24 next-hop 1.1.1.3
set routing-instances vr0 routing-options static route 66.66.66.0/24 next-hop 1.1.1.5
```

Step-by-Step Procedure

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

To configure the master logical system interfaces:

1. Configure the master (root) logical system and lt-0/0/0.1 interfaces.

```
[edit interfaces]
user@host# set ge-5/0/0 vlan-tagging
user@host# set ge-5/0/0 unit 0 vlan-id 600
user@host# set lt-0/0/0 unit 1 encapsulation Ethernet
user@host# set lt-0/0/0 unit 1 peer-unit 0
user@host# set lt-0/0/0 unit 1 family inet address 1.1.1.1/24
user@host# set lt-0/0/0 unit 1 family inet6 address 1111::1/64
user@host# set ge-5/0/0 unit 0 family inet address 99.99.99.1/24
user@host# set ge-5/0/0 unit 0 family inet6 address 9999::1/64
```

2. Configure a routing instance for the master logical system, assign its interfaces to it, and configure static routes for it.

```
[edit interfaces routing-instances]
user@host# set vr0 instance-type virtual-router
user@host# set vr0 interface lt-0/0/0.1
user@host# set vr0 interface ge-5/0/0.0
user@host# set vr0 routing-options rib vr0.inet6.0 static route 7777::/64 next-hop
  1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 8888::/64 next-hop
  1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 6666::/64 next-hop
  1111::5
user@host# set vr0 routing-options static route 77.77.77.0/24 next-hop 1.1.1.3
user@host# set vr0 routing-options static route 88.88.88.0/24 next-hop 1.1.1.3
user@host# set vr0 routing-options static route 66.66.66.0/24 next-hop 1.1.1.5
```

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 instructions in this example to correct the configuration.

```
[edit]
user@host# show interfaces
ge-5/0/0 {
   vlan-tagging;
   unit 0 {
      vlan-id 600;
      family inet {
         address 99.99.99.1/24;
      }
      family inet 6{
         address 9999::1/64;
      }
   }
}
lt-0/0/0 {
   unit 1 {
      encapsulation ethernet;
```

```
    peer-unit 0;
    family inet {
      address 1.1.1.1/24;
    }
    family inet 6{
      address 1111::1/64;
    }
  }
}
```

```
[edit]
user@host# show routing-instances
vr0 {
  instance-type virtual-router;
  interface ge-5/0/0.0;
  interface lt-0/0/0;
  routing-options {
    rib vr0.inet6.0 {
    static {
      route 8888::/64 next-hop 1111::3;
      route 7777::/64 next-hop 1111::3;
      route 6666::/64 next-hop 1111::5;
    }
    }
    static {
      route 77.77.77.0/24 next-hop 1.1.1.3;
      route 88.88.88.0/24 next-hop 1.1.1.3;
      route 66.66.66.0/24 next-hop 1.1.1.5;
    }
  }
}
```

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

Configuring Logical Tunnel Interfaces for the User Logical Systems

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 logical-systems LSYS1 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 peer-unit 2
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet address 1.1.1.3/24
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet6 address 1111::3/64
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 peer-unit 4
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet address 1.1.1.5/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet6 address 1111::5/64
```

Step-by-Step Procedure

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

1. Configure the lt-0/0/0 interface for the first user logical system:

```
[edit logical-systems LSYS1 interfaces lt-0/0/0 unit 3]
user@host# set encapsulation ethernet
user@host# set peer-unit 2
user@host# set family inet address 1.1.1.3/24
user@host# set family inet6 address 1111::3/64
```

2. Configure the lt-0/0/0 interface for the second user logical system.

```
[edit logical-systems LSYS2 interfaces lt-0/0/0 unit 5]
user@host# set encapsulation ethernet
user@host# set peer-unit 4
user@host# set family inet address 1.1.1.5/24
user@host# set family inet6 address 1111::5/64
```

Results From configuration mode, confirm your configuration by entering the **show logical-systems LSYS1 interfaces lt-0/0/0**, and **show logical-systems LSYS2 interfaces lt-0/0/0** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host#  show logical-systems LSYS1 interfaces lt-0/0/0

lt-0/0/0 {
  unit 3 {
    encapsulation ethernet;
    peer-unit 2;
    family inet {
      address 1.1.1.3/24;
    }
    family inet 6{
      address 1111::3/64;
    }
  }
}

user@host#  show logical-systems LSYS2 interfaces lt-0/0/0

lt-0/0/0 {
  unit 5 {
    encapsulation ethernet;
    peer-unit 4;
    family inet {
      address 1.1.1.5/24;
    }
    family inet 6{
      address 1111::5/64;
    }
  }
}
```

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

Verification

Verifying That the Static Routes Configured for the Master Administrator Are Correct

Purpose Confirm that the configuration is working properly. Verify if you can send data from the master logical system to the other logical systems.

Action From operational mode, use the **ping** command.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding the Master Logical System and the Master Administrator Role on page 8
- Understanding User Logical Systems and the User Logical System Administrator Role on page 9
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces on page 10
- Example: Configuring IPv6 Zones for a User Logical System on page 234
- Example: Configuring IPv6 Security Policies for a User Logical System on page 237

Example: Configuring IPv6 Zones for a User Logical System

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 86.

- 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" on page 26

This example creates the IPv6 zones and address books described in Table 22 on page 235.

Table 22: 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
```

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 {
```

```
    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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Zones on page 95
- User Logical System Configuration Overview on page 86
- Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems on page 226
- Example: Configuring IPv6 Security Policies for a User Logical System on page 237

Example: Configuring IPv6 Security Policies for a User Logical System

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

- Requirements on page 238
- Overview on page 238
- Configuration on page 238
- Verification on page 240

Requirements

Before you begin:

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

  See "User Logical System Configuration Overview" on page 86.

- Use the **show system security-profiles policy** command to see the security policy resources allocated to the logical system.

  See the *Junos OS CLI Reference*.

- Configure zones and address books.

  See "Example: Configuring IPv6 Zones for a User Logical System" on page 234

Overview

This example shows how to configure the security policies described in Table 23 on page 238.

Table 23: 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
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 in the *Junos OS CLI User Guide*.

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
   ```

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Logical System Security Policies on page 102
- User Logical System Configuration Overview on page 86
- Troubleshooting Security Policies in the *Junos OS Security Configuration Guide*
- Example: Configuring IPv6 Zones for a User Logical System on page 234
- Example: Configuring IPv6 for the Master, Interconnect, and User Logical Systems on page 226

IPv6 Dual-Stack Lite

Understanding IPv6 Dual-Stack Lite in Logical Systems

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Configuring IPv6 Dual-Stack Lite for a User Logical System on page 242
- Understanding Logical Systems Security Profiles on page 34
- Understanding IPv6 Dual-Stack Lite in the *Junos OS Security Configuration Guide*

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

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 86.
- 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. See the *Junos OS CLI Reference*.

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" on page 26. 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 in the *Junos OS CLI User Guide*.

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
```

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

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding IPv6 Dual-Stack Lite in Logical Systems on page 241
- User Logical System Configuration Overview on page 86

PART 3

Monitoring and Troubleshooting

CHAPTER 6

Monitoring and Troubleshooting

Understanding Security Logs and Logical Systems

Security logs are system log messages that include security events. If a device is configured for logical systems, security logs generated within the context of a logical system use the name ***logname*_LS** (for example, **IDP_ATTACK_LOG_EVENT_LS**). The logical system version of a log has the same set of attributes as the log for devices that are not configured for logical systems, but it also includes logical-system-name as the first attribute.

The following security log shows the attributes for the IDP_ATTACK_LOG_EVENT log for a device that is *not* configured for logical systems:

```
IDP_ATTACK_LOG_EVENT {
  help "IDP attack log";
  description "IDP Attack log generated for attack";
  type event;
  args timestamp message-type source-address source-port destination-address
destination-port protocol-name service-name application-name rule-name
rulebase-name policy-name repeat-count action threat-severity attack-name
nat-source-address nat-source-port nat-destination-address nat-destination-port
elapsed-time inbound-bytes outbound-bytes inbound-packets outbound-packets
source-zone-name source-interface-name destination-zone-name
destination-interface-name packet-log-id message;
  severity LOG_INFO;
  flag auditable;
  edit "2010/10/01 mvr created";
}
```

The following security log shows the attributes for the IDP_ATTACK_LOG_EVENT_LS log for a device that is configured for logical systems (note that logical-system-name is the first attribute):

```
IDP_ATTACK_LOG_EVENT_LS {
  help "IDP attack log";
  description "IDP Attack log generated for attack";
  type event;
  args logical-system-name timestamp message-type source-address source-port
```

```
destination-address destination-port protocol-name service-name application-name
rule-name rulebase-name policy-name repeat-count action threat-severity attack-name
 nat-source-address nat-source-port nat-destination-address nat-destination-port
elapsed-time inbound-bytes outbound-bytes inbound-packets outbound-packets
source-zone-name source-interface-name destination-zone-name
destination-interface-name packet-log-id message;
  severity LOG_INFO;
  flag auditable;
  edit "2010/10/01 mvr created";
}
```

If a device is configured for logical systems, log parsing scripts might need to be modified because the log name includes the **_LS** suffix and the logical-system-name attribute can be used to segregate logs by logical system.

If a device is not configured for logical systems, the security logs remain unchanged and scripts built to parse logs do not need any modification.

NOTE: **Only the master administrator can configure logging at the [edit security log] hierarchy level. User logical system administrators cannot configure logging for their logical systems.**

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- System Log Messages Overview in the *Junos OS Monitoring and Troubleshooting Guide for Security Devices*
- Configuring System Log Messages in the *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

Understanding Data Path Debugging for Logical Systems

Data path debugging provides tracing and debugging at multiple processing units along the packet-processing path. Data path debugging can also be performed on traffic between logical systems.

NOTE: **Only the master administrator can configure data path debugging for logical systems at the [edit security datapath-debug] level. User logical system administrators cannot configure data path debugging for their logical systems.**

End-to-end event tracing traces the path of a packet from when it enters the device to when it leaves the device. When the master administrator configures end-to-end event tracing, the trace output contains logical system information.

The master administrator can also configure tracing for traffic between logical systems. The trace output shows traffic entering and leaving the logical tunnel between logical systems. When the **preserve-trace-order** option is configured, the trace message is sorted

chronologically. In addition to the trace action, other actions such as packet-dump and packet-summary may be configured for traffic between logical systems.

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Performing Tracing for Logical Systems on page 249
- Understanding Data Path Debugging for SRX Series Devices in the *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

Performing Tracing for Logical Systems

NOTE: Only the master administrator can configure data path debugging for logical systems at the root level.

To configure an action profile for a trace or packet capture:

1. Specify event types and trace actions. You can specify any combination of event types and trace actions. For example, the following statements configure multiple trace actions for each event type:

```
[edit security datapath-debug]
user@host# set action-profile p1 event lbt trace
user@host# set action-profile p1 event lbt count
user@host# set action-profile p1 event lbt packet-summary
user@host# set action-profile p1 event lbt packet-dump
user@host# set action-profile p1 event pot trace
user@host# set action-profile p1 event pot count
user@host# set action-profile p1 event pot packet-summary
user@host# set action-profile p1 event pot packet-dump
user@host# set action-profile p1 event np-ingress trace
user@host# set action-profile p1 event np-ingress count
user@host# set action-profile p1 event np-ingress packet-summary
user@host# set action-profile p1 event np-ingress packet-dump
user@host# set action-profile p1 event np-egress trace
user@host# set action-profile p1 event np-egress count
user@host# set action-profile p1 event np-egress packet-summary
user@host# set action-profile p1 event np-egress packet-dump
user@host# set action-profile p1 event jexec trace
user@host# set action-profile p1 event jexec count
user@host# set action-profile p1 event jexec packet-summary
user@host# set action-profile p1 event jexec packet-dump
user@host# set action-profile p1 event lt-enter trace
user@host# set action-profile p1 event lt-enter count
user@host# set action-profile p1 event lt-enter packet-summary
user@host# set action-profile p1 event lt-enter packet-dump
user@host# set action-profile p1 event lt-leave trace
user@host# set action-profile p1 event lt-leave count
user@host# set action-profile p1 event lt-leave packet-summary
user@host# set action-profile p1 event lt-leave packet-dump
```

2. Specify action profile options.

```
[edit security datapath-debug]
user@host# set action-profile p1 record-pic-history
user@host# set action-profile p1 preserve-trace-order
```

3. Configure packet filter options.

```
[edit security datapath-debug]
user@host# set packet-filter 1 action-profile p1
user@host# set packet-filter 1 protocol udp
```

To capture trace messages for logical systems:

1. Configure the trace capture file.

```
[edit security datapath-debug]
user@host# set traceoptions file e2e.trace
user@host# set traceoptions file size 10m
```

2. Display the captured trace in operational mode.

```
user@host> show log e2e.trace
  Jul  7 09:49:56
  09:49:56.417578:CID-00:FPC-01:PIC-00:THREAD_ID-00:FINDEX:0:IIF:75:SEQ:0:TC:0
  PIC History: ->C0/F1/P0
  NP ingress channel 0 packet
  Meta: Src: F1/P0 Dst: F0/P0
  IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500

  Jul  7 09:49:56
  09:49:55.1414031:CID-00:FPC-00:PIC-00:THREAD_ID-04:FINDEX:0:IIF:75:SEQ:0:TC:1
  PIC History: ->C0/F1/P0->C0/F0/P0
  LBT pkt, payload: DATA
  Meta: Src: F1/P0 Dst: F0/P0
  IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500

  ...
  (Some trace information omitted)
  ...

  .Jul  7 09:49:56
  09:49:55.1415649:CID-00:FPC-00:PIC-00:THREAD_ID-05:FINDEX:0:IIF:75:SEQ:0:TC:16
  PIC History: ->C0/F1/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0
  POT pkt, action: POT_SEND payload: DATA
  Meta: Src: F0/P0 Dst: F1/P0
  IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500

  Jul  7 09:49:56
  09:49:56.419274:CID-00:FPC-01:PIC-00:THREAD_ID-00:FINDEX:0:IIF:75:SEQ:0:TC:17
  PIC History:
  ->C0/F1/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F0/P0->C0/F1/P0
  NP egress channel 0 packet
  Meta: Src: F0/P0 Dst: F1/P0
  IP: saddr 10.1.1.2 daddr 30.1.1.2 proto 6 len 500
```

3. Clear the log.

```
user@host> clear log e2e.trace
```

To perform packet capture for logical systems:

1. Configure the packet capture file.

```
[edit security datapath-debug]
user@host# set capture-file e2e.pcap
user@host# set capture-file format pcap
user@host# set capture-file size 10m
user@host# set capture-file world-readable
user@host# set capture-file maximum-capture-size 1500
```

2. Enter operational mode to start and then stop the packet capture.

```
user@host> request security datapath-debug capture start
user@host> request security datapath-debug capture stop
```

NOTE: Packet capture files can be opened and analyzed offline with tcpdump or any packet analyzer that recognizes the libpcap format. You can also use FTP or the Session Control Protocol (SCP) to transfer the packet capture files to an external device.

3. Disable packet capture from configuration mode.

NOTE: Disable packet capture before opening the file for analysis or transferring the file to an external device with FTP or SCP. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

```
[edit forwarding-options]
user@host# set packet-capture disable
```

4. Display the packet capture.

   - To display the packet capture with the tcpdump utility:

```
user@host# tcpdump -nr /var/log/e2e.pcap
  09:49:55.1413990 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1414154 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
  S 0:460(460) win 0
  09:49:55.1415062 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1415184 C0/F0/P0 event:11(lbt) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
  S 0:460(460) win 0
  09:49:55.1414093 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1414638 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1415011 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1415129 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
  09:49:55.1415511 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
   S 0:460(460) win 0
```

```
09:49:55.1415649 C0/F0/P0 event:12(pot) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
 S 0:460(460) win 0
09:49:55.1415249 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
 S 0:460(460) win 0
09:49:55.1415558 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
 S 0:460(460) win 0
09:49:55.1414226 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
 S 0:460(460) win 0
09:49:55.1414696 C0/F0/P0 event:18(jexec) SEQ:0 IP 10.1.1.2.23451 > 30.1.1.2.12345:
 S 0:460(460) win 0
09:49:55.1414828 C0/F0/P0 event:16(lt-enter) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:55.1414919 C0/F0/P0 event:15(lt-leave) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:56.417560 C0/F1/P0 event:1(np-ingress) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
09:49:56.419263 C0/F1/P0 event:2(np-egress) SEQ:0 IP 10.1.1.2.23451 >
30.1.1.2.12345: S 0:460(460) win 0
```

- To display the packet capture from CLI operational mode:

```
user@host> show security datapath-debug capture
  Packet 1, len 568: (C0/F0/P0/SEQ:0:lbt)
  00 00 00 00 00 00 50 c5 8d 0c 99 4a 00 00 0a 01
  01 02 08 00 45 60 01 f4 00 00 00 00 40 06 4e 9f
  0a 01 01 02 1e 01 01 02 5b 9b 30 39 00 00 00 00
  00 00 00 00 50 02 00 00 f8 3c 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 ac 7a 00 04
  00 00 00 00 b3 e3 15 4e 66 93 15 00 04 22 38 02
  38 02 00 00 00 01 00 03 0b 00 00 00 50 d0 1a 08
  30 de be bf e4 f3 19 08
  Packet 2, len 624: (C0/F0/P0/SEQ:0:lbt)
  aa 35 00 00 00 00 00 00 00 00 00 00 03 00 00
  00 0a 00 00 00 00 00 00 05 bd 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 c5
  8d 0c 99 4a 00 00 0a 01 01 02 08 00 45 60 01 f4
  00 00 00 00 40 06 4e 9f 0a 01 01 02 ac 7a 00 04
  00 00 00 00 b3 e3 15 4e 0a 94 15 00 04 5a 70 02
  70 02 00 00 00 03 00 03 0b 00 00 00 50 d0 1a 08
  30 de be bf e4 f3 19 08

  ...
  (Packets 3 through 17 omitted)
  ...

  Packet 18, len 568: (C0/F1/P0/SEQ:0:np-egress)
  00 00 00 04 00 00 00 00 1e 01 01 02 50 c5 8d 0c
  99 4b 08 00 45 60 01 f4 00 00 00 00 3e 06 50 9f
  0a 01 01 02 1e 01 01 02 5b 9b 30 39 00 00 00 00
  00 00 00 00 50 02 00 00 f8 3c 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 ac 7a 04 00
  00 00 00 00 b4 e3 15 4e bf 65 06 00 04 22 38 02
```

```
    38 02 00 00 00 11 00 03 02 00 00 00 50 d0 1a 08
    30 de be bf e4 f3 19 08

user@host> show security datapath-debug counters
    Datapath debug counters
    Packet Filter 1:
    lt-enter
    Chassis 0 FPC 0 PIC 1: 0
    lt-enter
    Chassis 0 FPC 0 PIC 0: 1
    lt-leave
    Chassis 0 FPC 0 PIC 1: 0
    lt-leave
    Chassis 0 FPC 0 PIC 0: 1
    np-egress
    Chassis 0 FPC 1 PIC 3: 0
    np-egress
    Chassis 0 FPC 1 PIC 1: 0
    np-egress
    Chassis 0 FPC 1 PIC 2: 0
    np-egress
    Chassis 0 FPC 1 PIC 0: 1
    pot
    Chassis 0 FPC 0 PIC 1: 0
    pot
    Chassis 0 FPC 0 PIC 0: 6
    np-ingress
    Chassis 0 FPC 1 PIC 3: 0
    np-ingress
    Chassis 0 FPC 1 PIC 1: 0
    np-ingress
    Chassis 0 FPC 1 PIC 2: 0
    np-ingress
    Chassis 0 FPC 1 PIC 0: 1
    lbt
    Chassis 0 FPC 0 PIC 1: 0
    lbt
    Chassis 0 FPC 0 PIC 0: 4
    jexec
    Chassis 0 FPC 0 PIC 1: 0
    jexec
    Chassis 0 FPC 0 PIC 0: 4
```

Related Documentation

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Data Path Debugging for Logical Systems on page 248
- Debugging the Data Path (CLI Procedure) in the *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

PART 4

Index

Index

Symbols

A

B

C

D

E

F

I

L

V

Z