JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Logical Systems and Tenant Systems User Guide for Security Devices

Published
2024-12-12

JUNOS

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

Junos® OS Logical Systems and Tenant Systems User Guide for Security Devices

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

Use this guide to configure logical systems and tenant Systems in Junos OS on the SRX Series Firewalls to partition a single device into multiple domains to perform security and routing functions.

CHAPTER 1

Overview

Logical Systems and Tenant Systems Overview

With the Junos operating system (Junos OS) on SRX Series Firewall, you can partition a single security device into multiple logical devices that can perform independent tasks. Because logical systems perform a subset of the tasks once handled by the main device, logical systems offer an effective way to maximize the use of a single security platform.

A complex network design requires multiple layers of switches, routers, and security devices, which might lead to challenges in maintenance, configuration, and operation. To reduce such complexity, Juniper Networks supports logical systems. Logical systems perform a subset of the actions of the main device and have their own unique routing tables, interfaces, policies, and routing instances.

For SRX Series Firewalls, you can partition a single device into following secure contexts:

- Logical systems
- Tenant systems

Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. A tenant system provides logical partitioning of the SRX Series Firewall into multiple domains similar to logical systems and provides high scalability.

2

CHAPTER

Logical Systems

Logical Systems Overview

IN THIS SECTION

Logical systems enable you to partition a single device into multiple secure contexts that perform independent tasks. For more information, see the following topics:

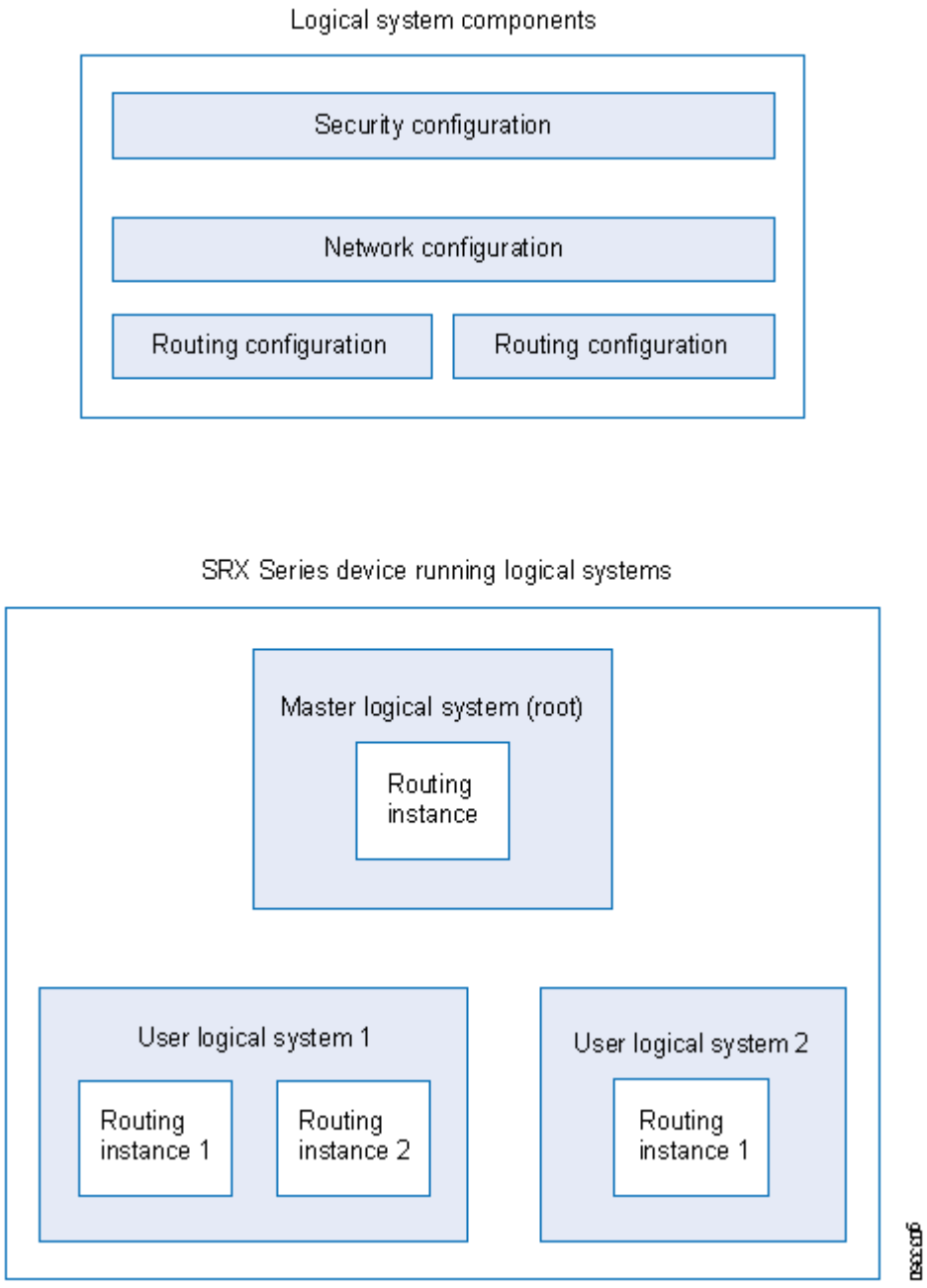
Understanding Logical Systems for SRX Series Firewalls

Logical systems for SRX Series Firewalls 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 Firewall 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 primary logical system.

The top part of Figure 1 on page 6 shows the three main configuration components of a logical system. The lower part of the figure shows a single device with a primary logical system and discrete user logical systems.

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

Figure 1: Understanding Logical Systems



Logical systems on SRX Series Firewalls 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 primary, 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 Firewall 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 Firewall running logical systems provides for high, fast interaction among all logical systems created on the device when an interconnect logical system is used.

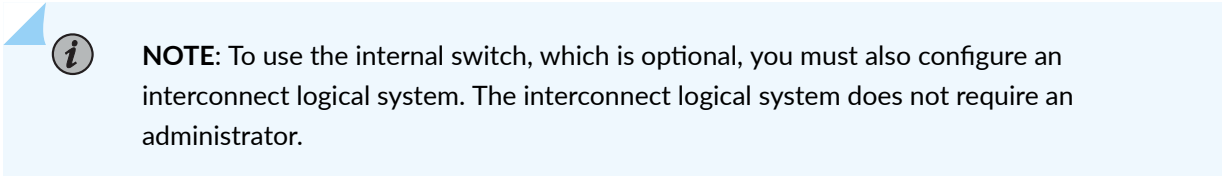
  Logical systems on the same device can also communicate with one another directly through ports on the device, as if they were separate devices. Although this method allows for direct connections between logical systems, it consumes more resources–you must configure interfaces and an external switch–and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

- In the data center, as a service provider, you can deploy an SRX Series Firewall 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.

- SRX4100 and SRX4200 devices support logical system in both transparent and route mode.

- SRX4600 device supports logical system in route mode only.



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.

SEE ALSO

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Features and Limitations of Logical Systems

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

- You can configure up to 32 security profiles, from 1 through 32, with ID 0 reserved for the internally configured default security profile. When the maximum number of security profiles is reached, if you want to add a new security profile, you must first delete one or more existing security profiles, commit the configuration, and then create the new security profile and commit it. You cannot add a new security profile and remove an existing one within a single configuration commit.

  If you want to add more than one new security profile, the same rule is true. You must first delete the equivalent number of of existing security profiles, commit the configuration, and then create the new security profiles and commit the configuration.

- You can configure one or more primary administrators to oversee administration of the device and the logical systems they configure.

  As primary 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 primary 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 primary administrator creates login accounts for these administrators and assigns them to a user logical system. Currently, the primary administrator must configure all user logical system administrators. The first assigned user logical administrator cannot configure additional user logical system administrators for his or her 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 primary 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.

- Commit rollback is supported at the root level only.

- Quality-of-service (QoS) classification across interconnected logical systems does not work.
- The primary administrator can configure Application Layer Gateways (ALGs) at the root level. The configuration is inherited by all user logical systems. ALGs can also be configured discretely for user logical systems.
- The primary administrator can configure IDP policies at the root level and then apply an IDP policy to a user logical system.
- Only the primary administrator can create user accounts and login IDs for users for all logical systems. The primary 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 primary administrator. A user logical system administrator cannot create other user logical system administrators or user accounts for their logical systems.
- Some of the scaling parameters are different for SRX1500 devices. For example, you can configure a maximum of 512 zones under a logical system.

SEE ALSO

Understanding Logical Systems for SRX Series Firewalls | 5

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding User Logical Systems and the User Logical System Administrator Role | 50

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 primary 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 Firewall running logical systems can be used in a *chassis cluster*. Each node has the same configuration, including the interconnect logical system.

SEE ALSO

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only) | **111**

Understanding Logical Systems for SRX Series Firewalls | **5**

Understanding Logical Systems in the Context of Chassis Cluster | **406**

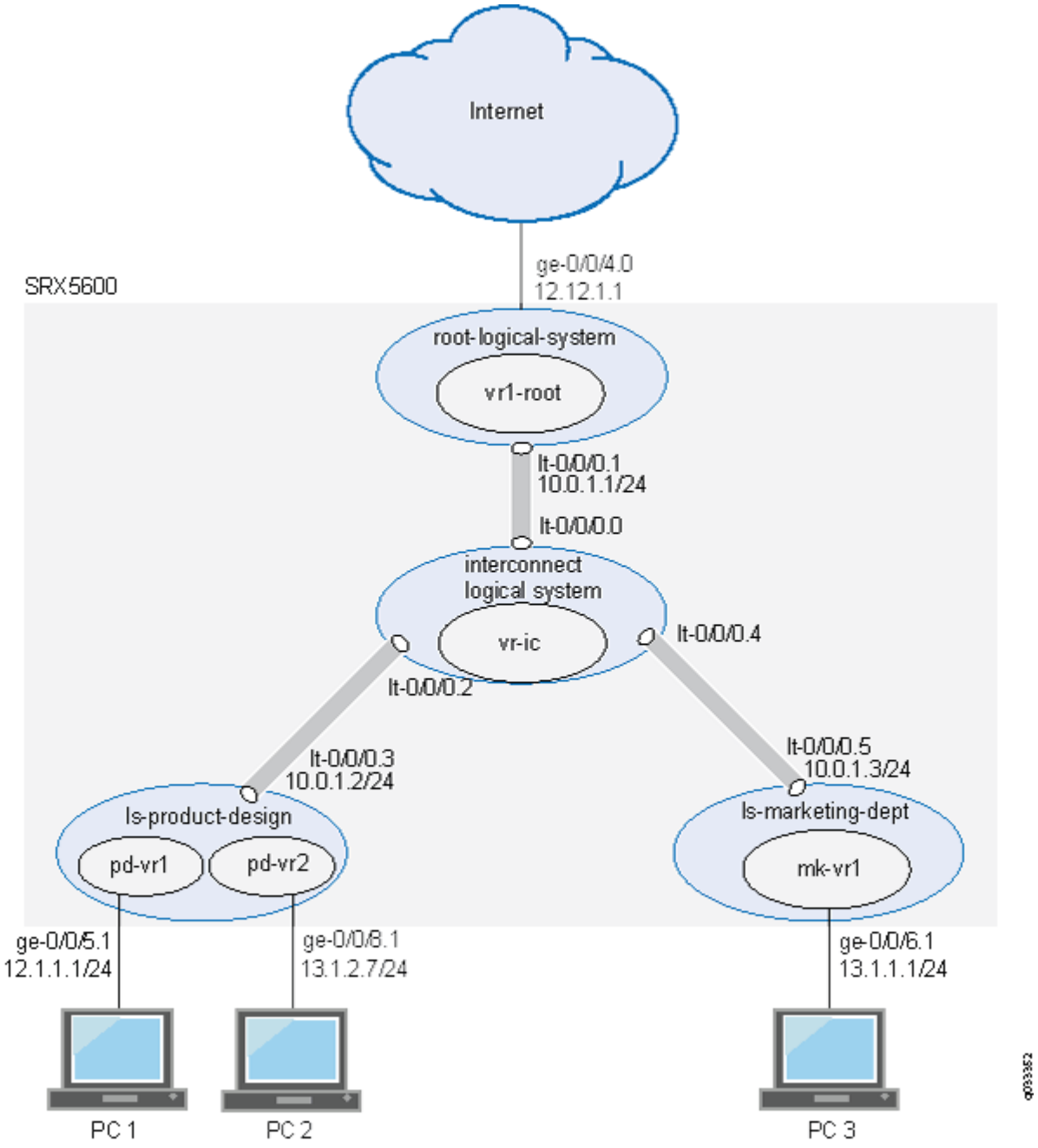
Understanding Packet Flow in Logical Systems for SRX Series Devices

IN THIS SECTION

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

The concepts explained in this example rely on the topology shown in Figure 2 on page 12.

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



Understanding Junos OS SRX Series Firewalls Architecture

Junos OS is a distributed parallel processing high throughput and high performance system. The distributed parallel processing architecture of the services gateways includes multiple processors to manage sessions and run security and other services processing. This architecture provides greater flexibility and allows for high throughput and fast performance.

The SRX5000 line devices include I/O cards (IOC) 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.

These processing units have different responsibilities. All flow-based services for a packet are executed on a single SPU. Otherwise, however, the lines are not clearly divided in regard to the kinds of services that run on these processors. (For details on flow-based processing, see *Understanding Traffic Processing on Security Devices*.)

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 in an intelligent way. The central point 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, including the central point, 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 if it belongs to an existing session.

This architecture allows the device to distribute processing of all sessions across multiple SPUs. It also allows an NPU to determine if a session exists for a packet, to check the packet, and to apply screens to it. How a packet is handled depends on whether it is the first packet of a flow.

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 Firewalls running logical systems differs in minor ways from that of SRX Series Firewalls 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 Firewalls 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 primary logical system in the same way as it is for user logical systems on the device.

NOTE: On SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 Series devices, J-Flow version 5, version 8, and version 9 are not supported on logical systems.

Understanding Packet Classification

Packet classification is assessed the same way for SRX Series Firewalls 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 Firewalls 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 Firewalls 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.

SEE ALSO

Understanding the Interconnect Logical System and Logical Tunnel Interfaces | 9

Understanding Logical Systems for SRX Series Firewalls | 5

Logical Systems and Tenant Systems support for vSRX Virtual Firewall and vSRX Virtual Firewall 3.0 Instances

Starting in Junos OS Release 20.1R1, you can configure logical systems and tenant systems on vSRX Virtual Firewall and vSRX Virtual Firewall 3.0 instances.

Configuring each logical systems creates an extra routing protocol process (RPD), which is cpu and memory intensive. Starting in Junos OS Release 20.1R1-

- vSRX Virtual Firewall and vSRX3.0 instances with a memory capacity of less than 16GB support one root logical system.
- vSRX Virtual Firewall and vSRX3.0 instances with a memory capacity of 16GB or more supports logical systems but limits the logical systems to eight.

Table 1 on page 20 describes the number of logical systems and tenant systems supported on different memory capacities for vSRX Virtual Firewall and vSRX Virtual Firewall 3.0.

Table 1: Logical Systems and Tenant Systems supported on different Memory Capacities for vSRX Virtual Firewall and vSRX Virtual Firewall 3.0.

Type	4GB	8GB	16GB or more
Logical systems (includes the root logical system)	1	1	8
Tenant systems	0	0	42
Logical systems + Tenant systems (includes the root logical system).	1	1	50

NOTE: Only vSRX Virtual Firewall 3.0 instances support flexible security profiles based on the device memory. The maximum number of supported security profiles on vSRX Virtual Firewall 3.0 is related to its memory. For more information, see Security Profiles for Logical Systems.

Use the following command at the `[edit]` hierarchy level to ensure that there are at least two CPUs in the Routing Engine of vSRX Virtual Firewall and vSRX3.0 instances: `set security forwarding-options resource-manager cpu re 2`.

SEE ALSO

- Logical Systems Overview
- Tenant Systems Overview

Primary Logical Systems Overview

IN THIS SECTION

Primary logical systems can create a user logical system and configure the security resources of the user logical system. Primary logical systems assign the logical interfaces to the user logical systems. For more information, see the following topics:

Understanding the Primary Logical Systems and the Primary Administrator Role

When, as a primary administrator, you initialize an SRX Series Firewall running logical systems, a primary 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 primary logical system, and the primary administrator allocates them to the user logical systems.

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

- The primary 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 primary logical system.

    Only the primary 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 primary administrator can also use trace and debug at the root level, and he can perform commit rollbacks. The primary administrator manages the primary 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.

SEE ALSO

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Understanding Logical Systems for SRX Series Firewalls | 5

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only) | 111

SRX Series Logical Systems Primary Administrator Configuration Tasks Overview

This topic describes the primary administrator's tasks in the order in which they are performed.

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

For an overview of the primary administrator's role and responsibilities, see "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

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

1. Configure a root password. Initially the primary 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 Root Password for Logical Systems" on page 52 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 primary 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 primary administrator must define and add all user logical system administrators and add them to their user logical systems.

   The primary 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.

   - For configuration information, see "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54
   - For information on user logical system administrators, see "Understanding User Logical Systems and the User Logical System Administrator Role" on page 50.
   - For information on the interconnect logical system, see "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 9.

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 (Primary Administrators Only)" on page 74.
   - For information on security profiles, see "Understanding Logical Systems Security Profiles (Primary Administrators Only)" on page 68.

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 primary 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 primary logical system and add its interfaces and static routes to it. Also configure logical interfaces for user logical systems with VLAN tagging.

> **NOTE**: The primary 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. VPLS is a virtual private network (VPN) technology. It allows point-to-point layer 2 tunnels connectivity.

  By creating a VPLS type routing-instance (RI), we define a VPLS switch. VPLS switch behaves like a L2 ethernet switch. We assign multiple LT IFLs to the VPLS switch. Each LT IFL have encapsulation ethernet-vpls and this behaves as L2 switch port. To connect to the VPLS switch, each logical system creates a LT IFL and assigns to a port of the VPLS switch.

  Starting with Junos OS Release 18.2R1, it is not required to define a dedicated interconnect logical system for including VPLS switch. For ease, VPLS switch is defined in root logical system. This approach is enabled by configuring multiple VPLS switches and LT IFLs per logical system.

  When one LT logical interface connects to a VPLS switch, the routing engine assigns VPLS switch unique MAC address from MAC address pool of the LT interface. This determines the number of LT IFLs that connect a VPLS switch.

- For configuration information, see "Routing and Interfaces for Primary Logical Systems" on page 111.

- 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 9.

5. Enable CPU utilization control and configure the CPU control target and reserved CPU quotas for logical systems. See "Example: Configuring CPU Utilization (Primary Administrators Only)" on page 105.
6. Optionally, configure dynamic routing protocols for the primary logical system. See "Example: Configuring OSPF Routing Protocol for the Primary Logical Systems" on page 123
7. Configure zones, security policies, and security features for the primary logical system. See "Example: Configuring Security Features for the Primary Logical Systems" on page 172.
8. Configure IDP for the primary logical system. See "Example: Configuring an IDP Policy for the Primary Logical Systems" on page 276.
9. Configure application firewall services on the primary logical system. See "Understanding Logical Systems Application Firewall Services" on page 337 and "Example: Configuring Application Firewall Services for a Primary Logical Systems" on page 338.

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 (Primary Administrators Only)" on page 231.

SEE ALSO

Understanding Logical Systems for SRX Series Firewalls | 5

Example: Configuring Multiple VPLS Switches and LT Interfaces for Logical Systems

IN THIS SECTION

This example shows how to interconnect multiple logical systems. This is achieved by configuring multiple logical systems with a Logical Tunnel (LT) interface point-to-point connection (Encapsulation Ethernet, Encapsulation Frame-Relay and Virtual Private LAN Service switch). More than one LT interface under a logical system and multiple VPLS switches are configured to pass the traffic without leaving an SRX Series Firewall. The frame-relay encapsulation adds data-link connection identifier (DLCI) information to the given frame.

Requirements

This example uses an SRX Series Firewall running Junos OS with logical system.

Before you begin:

- Read the "SRX Series Logical Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how and where this procedure fits in the overall primary administrator configuration process.
- Read the "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54

- Read the "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 9

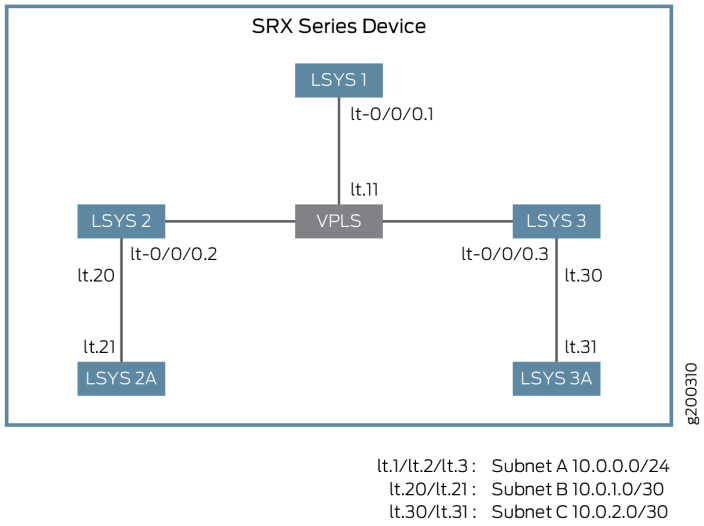
Overview

In this example, we configure multiple LT interfaces and multiple VPLS switches under one logical system.

In this example, we also configure interconnect multiple logical systems with LT interface point-to point connection (Encapsulation Ethernet and Encapsulation Frame-Relay).

Figure 3 on page 26 shows the topology for interconnecting logical systems.

Figure 3: Configuring the interconnect logical systems



- For the interconnect logical system with LT interface point-to-point connection (encapsulation ethernet), the example configures logical tunnel interfaces lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

  The interconnect logical systems lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the logical systems are configured with Ethernet as the encapsulation type. A security profile is assigned to the logical systems.

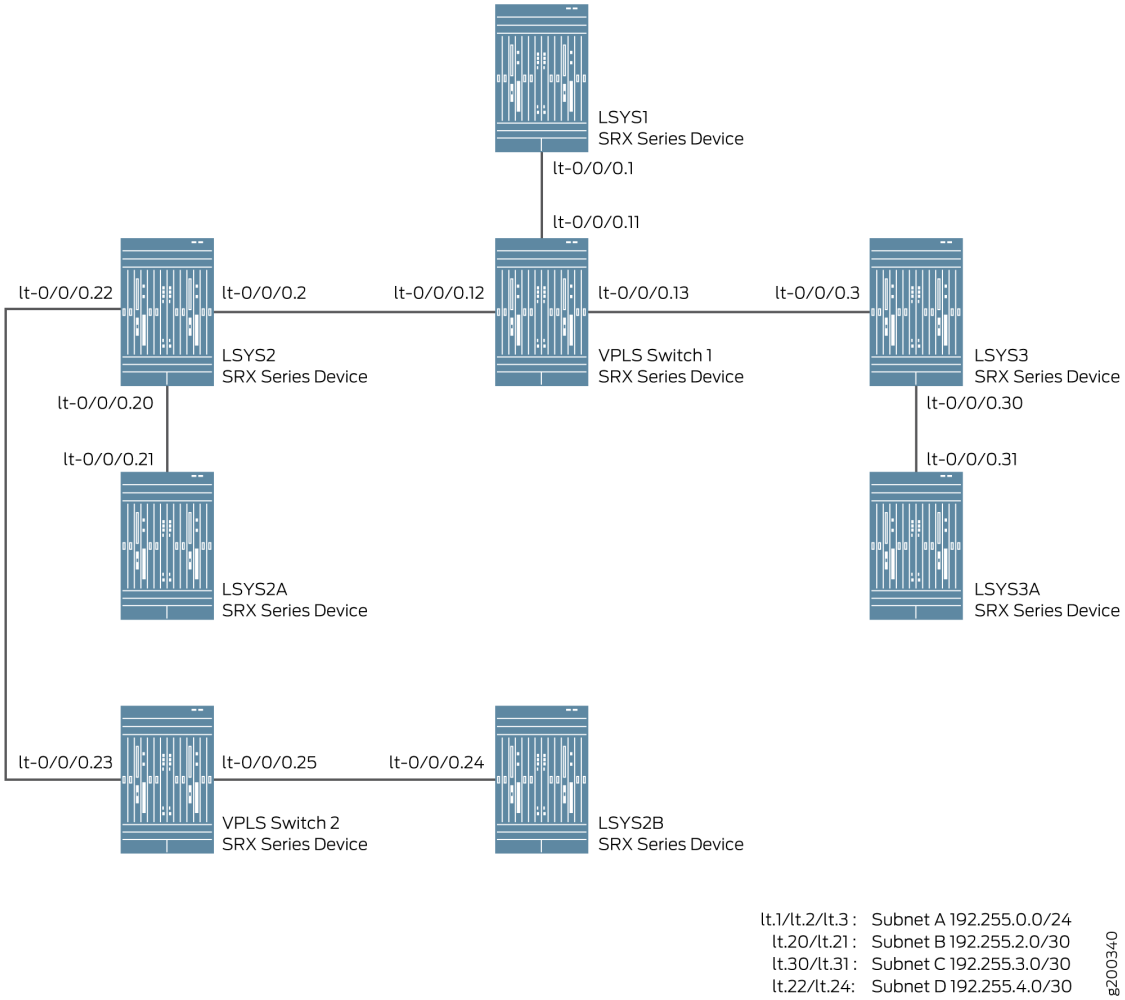
- For the interconnect logical systems with LT interface point-to-point connection (encapsulation frame-relay), this example configures logical tunnel interfaces lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

  The interconnect logical systems lt-0/0/0 interfaces are configured with frame-relay as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the logical systems are configured with frame-relay as the encapsulation type. A security profile is assigned to the logical systems.

- For interconnect logical systems with multiple VPLS switches, this example configures logical tunnel interfaces lt-0/0/0 with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces and security-profiles are assigned to the logical systems. The routing instance for the VPLS switch-1 and VPLS switch-2 are also assigned to the logical systems.

  Figure 4 on page 27 shows the topology for interconnect logical systems with VPLS switches.

Figure 4: Configuring the interconnect logical systems with VPLS switches



NOTE: Multiple LT interfaces can be configured within a logical system.

Configuration

IN THIS SECTION

To configure interfaces for the logical system, perform these tasks:

Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection (Encapsulation Ethernet)

CLI Quick Configuration

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

```
set system security-profile SP-user logical-system LSYS2
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 peer-unit 21
set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 family inet address 192.255.2.1/30
set logical-systems LSYS2 security zones security-zone LT interfaces lt-0/0/0.20
set system security-profile SP-user logical-system LSYS2A
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 encapsulation ethernet
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 peer-unit 20
set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 family inet address 192.255.2.2/30
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match source-
address any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match destination-
address any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT match application
any
set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT then permit
set logical-systems LSYS2A security policies default-policy permit-all
```

```
set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic system-services
all
set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic protocols all
set logical-systems LSYS2A security zones security-zone LT interfaces lt-0/0/0.21
```

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. Define a security profile and assign to a logical system.

```
[edit]
user@host# set system security-profile SP-user logical-system LSYS2
```

2. Set the LT interface as encapsulation ethernet in the logical system.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 encapsulation ethernet
```

3. Configure a peer relationship for logical systems LSYS2.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 peer-unit 21
```

4. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 20 family inet address
192.255.2.1/30
```

5. Set the security zone for the LT interface.

```
[edit]
user@host# set logical-systems LSYS2 security zones security-zone LT interfaces lt-0/0/0.20
```

6. Define a security profile and assign to a logical system.

```
[edit]
user@host# set system security-profile SP-user logical-system LSYS2A
```

7. Set the LT interface as encapsulation ethernet in the logical system 2A.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 encapsulation ethernet
```

8. Configure a peer relationship for logical systems LSYS2A.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 peer-unit 20
```

9. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS2A interfaces lt-0/0/0 unit 21 family inet address
192.255.2.2/30
```

10. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT
match source-address any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT
match destination-address any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT
match application any
user@host# set logical-systems LSYS2A security policies from-zone LT to-zone LT policy LT
then permit
```

11. Configure a security policy that permits traffic from default-policy.

```
[edit]
user@host# set logical-systems LSYS2A security policies default-policy permit-all
```

12. Configure security zones.

```
[edit]
user@host# set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic
system-services all
user@host# set logical-systems LSYS2A security zones security-zone LT host-inbound-traffic
protocols all
user@host# set logical-systems LSYS2A security zones security-zone LT interfaces
lt-0/0/0.21
```

Results

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2` 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 LSYS2
interfaces {
    lt-0/0/0 {
        unit 20 {
            encapsulation ethernet;
            peer-unit 21;
            family inet {
                address 192.255.2.1/30;
            }
        }
        unit 22 {
            encapsulation ethernet;
            peer-unit 23;
            family inet {
                address 192.255.4.1/30;
            }
        }
    }
```

```
}
security {
    zones {
        security-zone LT {
            interfaces {
                lt-0/0/0.22;
                lt-0/0/0.20;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2A` 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 LSYS2A
interfaces {
    lt-0/0/0 {
        unit 21 {
            encapsulation ethernet;
            peer-unit 20;
            family inet {
                address 192.255.2.2/30;
            }
        }
    }
}
security {
    policies {
        from-zone LT to-zone LT {
            policy LT {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
```

```
        }
        default-policy {
            permit-all;
        }
    }
    zones {
        security-zone LT {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lt-0/0/0.21;
            }
        }
    }
}
```

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

Configuring Logical Systems Interconnect with Logical Tunnel Interface point-to-point connection (Encapsulation Frame-Relay)

CLI Quick Configuration

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

```
set system security-profile SP-user logical-system LSYS3A
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 encapsulation frame-relay
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 dlci 16
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 peer-unit 31
set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 family inet address 192.255.3.1/30
set logical-systems LSYS3 security zones security-zone LT interfaces lt-0/0/0.30
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 encapsulation frame-relay
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 dlci 16
```

```
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 peer-unit 30
set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 family inet address 192.255.3.2/30
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match source-
address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match destination-
address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match application
any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT then permit
set logical-systems LSYS3A security policies default-policy permit-all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic system-services
all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic protocols all
set logical-systems LSYS3A security zones security-zone LT interfaces lt-0/0/0.31
```

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*.

1. Define a security profile and assign to a logical system.

```
[edit]
user@host# set system security-profile SP-user logical-system LSYS3A
```

2. Set the LT interface as encapsulation frame-relay in the logical system.

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 encapsulation frame-relay
```

3. Configure the logical tunnel interface by including the dlci.

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 dlci 16
```

4. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 peer-unit 31
```

5. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 30 family inet address
192.255.3.1/30
```

6. Set the security zone for the LT interface.

```
[edit]
user@host# set logical-systems LSYS3 security zones security-zone LT interfaces lt-0/0/0.30
```

7. Set the LT interface as encapsulation frame-relay in the logical system.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 encapsulation frame-relay
```

8. Configure the logical tunnel interface by including the dlci.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 dlci 16
```

9. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 peer-unit 30
```

10. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 31 family inet address
192.255.3.2/30
```

11. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match source-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match destination-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match application any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
then permit
```

12. Configure a security policy that permits traffic from default-policy.

```
[edit]
user@host# set logical-systems LSYS3A security policies default-policy permit-all
```

13. Configure security zones.

```
[edit]
user@host# set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
system-services all
user@host# set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
protocols all
user@host# set logical-systems LSYS3A security zones security-zone LT interfaces
lt-0/0/0.31
```

Results

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS3` commands. 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 LSYS3
interfaces {
    lt-0/0/0 {
        unit 30 {
            encapsulation frame-relay;
            dlci 16;
            peer-unit 31;
            family inet {
                address 192.255.3.1/30;
            }
        }
    }
}
security {
    zones {
        security-zone LT {
            interfaces {
                lt-0/0/0.30;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS3A` commands. 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 LSYS3A
```

```
    interfaces {
        lt-0/0/0 {
            unit 31 {
```

```
                encapsulation frame-relay;
                dlci 16;
                peer-unit 30;
                family inet {
                    address 192.255.3.2/30;
                }
            }
        }
    }
    security {
        policies {
            from-zone LT to-zone LT {
                policy LT {
                    match {
                        source-address any;
                        destination-address any;
                        application any;
                    }
                    then {
                        permit;
                    }
                }
            }
            default-policy {
                permit-all;
            }
        }
        zones {
            security-zone LT {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
                interfaces {
                    lt-0/0/0.31;
                }
            }
```

```
        }
    }
```

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

Configuring Logical Systems Interconnect with Multiple VPLS Switches

CLI Quick Configuration

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

```
set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 11 peer-unit 1
set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 12 peer-unit 2
set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 13 peer-unit 3
set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 23 peer-unit 22
set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 25 peer-unit 24
set routing-instances vpls-switch-1 instance-type vpls
set routing-instances vpls-switch-1 interface lt-0/0/0.11
set routing-instances vpls-switch-1 interface lt-0/0/0.12
set routing-instances vpls-switch-1 interface lt-0/0/0.13
set routing-instances vpls-switch-2 instance-type vpls
set routing-instances vpls-switch-2 interface lt-0/0/0.23
set routing-instances vpls-switch-2 interface lt-0/0/0.25
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 192.255.0.1/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 peer-unit 12
set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 family inet address 192.255.0.2/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 peer-unit 23
set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 family inet address 192.255.4.1/30
set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 encapsulation ethernet
set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 peer-unit 13
```

```
set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 family inet address 192.255.0.3/24
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 encapsulation ethernet
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 peer-unit 25
set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 family inet address 192.255.4.2/30
set system security-profile SP-user policy maximum 100
set system security-profile SP-user policy reserved 50
set system security-profile SP-user zone maximum 60
set system security-profile SP-user zone reserved 10
set system security-profile SP-user flow-session maximum 100
set system security-profile SP-user flow-session reserved 50
set system security-profile SP-user logical-system LSYS1
set system security-profile SP-user logical-system LSYS2
set system security-profile SP-user logical-system LSYS3
set system security-profile SP-user logical-system LSYS2B
```

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*.

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

```
[edit]
user@host# set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 11 peer-unit 1
user@host# set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 12 peer-unit 2
user@host# set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 13 peer-unit 3
user@host# set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 23 peer-unit 22
user@host# set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 25 peer-unit 24
```

2. Configure the routing instance for the VPLS switches and add interfaces to it.

```
[edit]
user@host# set routing-instances vpls-switch-1 instance-type vpls
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.11
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.12
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.13
```

```
user@host# set routing-instances vpls-switch-2 instance-type vpls
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.23
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.25
```

3. Configure LSYS1 with lt-0/0/0.1 interface and peer lt-0/0/0.11.

```
[edit]
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address
192.255.0.1/24
```

4. Configure LSYS2 with lt-0/0/0.2 interface and peer lt-0/0/0.12.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 encapsulation ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 peer-unit 12
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 2 family inet address
192.255.0.2/24
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 encapsulation ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 peer-unit 23
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 22 family inet address
192.255.4.1/30
```

5. Configure LSYS3 with lt-0/0/0.3 interface and peer lt-0/0/0.13

```
[edit]
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 encapsulation ethernet
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 peer-unit 13
user@host# set logical-systems LSYS3 interfaces lt-0/0/0 unit 3 family inet address
192.255.0.3/24
```

6. Configure LSYS2B with lt-0/0/0 interface and peer-unit 24.

```
[edit]
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 encapsulation ethernet
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 peer-unit 25
```

```
user@host# set logical-systems LSYS2B interfaces lt-0/0/0 unit 24 family inet address
192.255.4.2/30
```

7. Assign security-profile for logical-systems.

```
[edit]
user@host# set system security-profile SP-user policy maximum 100
user@host# set system security-profile SP-user policy reserved 50
user@host# set system security-profile SP-user zone maximum 60
user@host# set system security-profile SP-user zone reserved 10
user@host# set system security-profile SP-user flow-session maximum 100
user@host#set system security-profile SP-user flow-session reserved 50
user@host# set system security-profile SP-user logical-system LSYS1
user@host# set system security-profile SP-user logical-system LSYS2
user@host# set system security-profile SP-user logical-system LSYS3
user@host# set system security-profile SP-user logical-system LSYS2B
```

Results

- From configuration mode, confirm your configuration by entering the `show interfaces lt-0/0/0`, command. 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 11 {
    encapsulation ethernet-vpls;
    peer-unit 1;
}
unit 12 {
    encapsulation ethernet-vpls;
    peer-unit 2;
}
unit 13 {
    encapsulation ethernet-vpls;
    peer-unit 3;
}
unit 23 {
    encapsulation ethernet-vpls;
    peer-unit 22;
```

```
}
unit 25 {
    encapsulation ethernet-vpls;
    peer-unit 24;
}
```

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

```
[edit]
user@host# show routing-instances
vpls-switch-1 {
    instance-type vpls;
    interface lt-0/0/0.11;
    interface lt-0/0/0.12;
    interface lt-0/0/0.13;
}
vpls-switch-2 {
    instance-type vpls;
    interface lt-0/0/0.23;
    interface lt-0/0/0.25;
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1`, 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 LSYS1
interfaces {
    lt-0/0/0 {
        unit 1 {
            encapsulation ethernet;
            peer-unit 11;
            family inet {
                address 192.255.0.1/24;
            }
        }
```

```
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2`, 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 LSYS2
interfaces {
    lt-0/0/0 {
        unit 2 {
            encapsulation ethernet;
            peer-unit 12;
            family inet {
                address 192.255.0.2/24;
            }
        }
        unit 22 {
            encapsulation ethernet;
            peer-unit 23;
            family inet {
                address 192.255.4.1/30;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS3`, 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 LSYS3
interfaces {
    lt-0/0/0 {
        unit 3 {
            encapsulation ethernet;
            peer-unit 13;
            family inet {
                address 192.255.0.3/24;
```

```
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2B`, 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 LSYS2B
interfaces {
    lt-0/0/0 {
        unit 24 {
            encapsulation ethernet;
            peer-unit 25;
            family inet {
                address 192.255.4.2/30;
            }
        }
    }
}
```

- 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 configuration instructions in this example to correct it.

```
[edit]
user@host# show system security-profile
SP-user {
    policy {
        maximum 100;
        reserved 50;
    }
    zone {
        maximum 60;
        reserved 10;
    }
    flow-session {
        maximum 100;
        reserved 50;
```

```
    }
    logical-system [ LSYS1 LSYS2 LSYS3 LSYS2B ];
}
```

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

Verification

IN THIS SECTION

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

Verifying the Security-Profile for all Logical-systems

Purpose

Verify security profile for each logical systems.

Action

From operational mode, enter the `show system security-profile security-log-stream-number logical-system all` command.

```
user@host> show system security-profile security-log-stream-number logical-system all
```

```
logical system name   security profile name       usage    reserved   maximum
root-logical-system   Default-Profile                2           0         2000
LSYS1                 SP-user                        1          10         60
LSYS2                 SP-user                        1          10         60
LSYS2B                SP-user                        1          10         60
LSYS3                 SP-user                        1          10         60
```

Meaning

The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Verifying the LT Interfaces for all Logical systems

Purpose

Verify interfaces for logical systems.

Action

From operational mode, enter the `show interfaces lt-0/0/0 terse` command.

```
user@host> show interfaces lt-0/0/0 terse
```

```
Interface               Admin Link Proto    Local                 Remote
lt-0/0/0                up    up
lt-0/0/0.1              up    up   inet     192.255.0.1/24
lt-0/0/0.2              up    up   inet     192.255.0.2/24
lt-0/0/0.3              up    up   inet     192.255.0.3/24
lt-0/0/0.11             up    up   vpls
lt-0/0/0.12             up    up   vpls
lt-0/0/0.13             up    up   vpls
lt-0/0/0.22             up    up   inet     192.255.4.1/30
lt-0/0/0.23             up    up   vpls
lt-0/0/0.24             up    up   inet     192.255.4.2/30
lt-0/0/0.25             up    up   vpls
lt-0/0/0.32767          up    up
```

Meaning

The output provides the status of LT interfaces. All the LT interfaces are up.

SEE ALSO

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

User Logical Systems Overview

IN THIS SECTION

A user logical system enables you to configure zones, security policies, logical interfaces and security resources assigned to its own user logical system. For more information, see the following topics:

User Logical Systems Configuration Overview

When the primary 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 primary 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 primary administrator:

   a. SSH to the management IP address configured on the device. Log in to the user logical system with the administrator login and password provided by the primary administrator.

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

      Starting in Junos OS Release 20.1R1, On SRX5400, SRX5600, and SRX5800 Series devices, Trusted Platform Module (TPM) supports only with SRX5K-RE3-128G Routing Engine (RE3). The

TPM chip enables by default. To use the TPM functionality in logical systems, you must configure Master-Encryption-key (MEK) at the root logical system only, and the user logical systems will inherit the same MEK to encrypt configuration hash and public key infrastructure (PKI) key-pairs. For more information on TPM, see *Using Trusted Platform Module to Bind Secrets on SRX Series Devices*.

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

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

2. Configure the logical interfaces assigned to the user logical system by the primary 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 Systems" on page 135.

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 Security Zones for a User Logical Systems" on page 163.

   b. Configure screen options at the zone level. See "Example: Configuring Screen Options for a User Logical Systems" on page 220.

   c. Configure security policies between zones in the user logical system. See "Example: Configuring Security Policies in a User Logical Systems" on page 212.

      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 primary administrator creates access profiles in the primary logical system. See "Example: Configuring Access Profiles (Primary Administrators Only)" on page 169.

      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 183.

   e. Configure a route-based VPN tunnel to secure traffic between a user logical system and a remote site. The primary 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 (Primary Administrators Only)" on page 231.

The user logical system administrator then configures a route-based VPN tunnel. See "Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems" on page 241.

f. Configure Network Address Translation (NAT). See "Example: Configuring Network Address Translation for a User Logical Systems" on page 130.

g. Configure and assigning a predefined IDP policy to the user logical system. The primary 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 and Assigning a Predefined IDP Policy for a User Logical System" on page 284.

   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 288.

h. Configure and enable an IDP policy at the user logical system. See "Example: Configuring an IDP Policy for a User Logical System" on page 292

i. Display or clear application system cache (ASC) entries. See "Understanding Logical Systems Application Identification Services" on page 335.

j. Configure application firewall services on a user logical system. See "Understanding Logical Systems Application Firewall Services" on page 337 and "Example: Configuring Application Firewall Services for a User Logical System" on page 345.

k. Configure the AppTrack application tracking tool. See "Example: Configuring AppTrack for a User Logical Systems" on page 351.

SEE ALSO

Example: Configuring User Logical Systems | **146**

Understanding User Logical Systems and the User Logical System Administrator Role | **50**

Understanding User Logical Systems and the User Logical System Administrator Role

Logical systems allow a primary administrator to partition an SRX Series Firewall into discrete contexts called user logical systems. User logical systems are self-contained, private contexts, separate both from one another and from the primary 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 primary 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 primary administrator has a global view of the device and access to all user logical systems. If necessary, the primary 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 primary 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 primary 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 primary 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.

SEE ALSO

Understanding Logical Systems for SRX Series Firewalls | 5

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only) | 111

Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68

Example: Configuring Logical Systems Security Profiles (Primary Administrators Only) | 74

Setting Up a Logical System

IN THIS SECTION

Example: Configuring Root Password for Logical Systems

IN THIS SECTION

Requirements

Before you begin, read "SRX Series Logical Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how this task fits into the overall configuration process.

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

Overview

IN THIS SECTION

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 primary administrator. The primary administrator has root privileges over the device.

Topology

Configuration

IN THIS SECTION

Configuring the Root Password

Step-by-Step Procedure

- Configure a root password for the device.

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

SEE ALSO

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding Logical Systems for SRX Series Firewalls | 5

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

IN THIS SECTION

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 primary 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 primary administrator, who will add the users.

Requirements

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

Overview

IN THIS SECTION

Before you begin, read "SRX Series Logical Systems Primary Administrator Configuration Tasks Overview" on page 22 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 primary administrator configures three user logical systems giving each department a logical device that is private and fully secured.

This topic covers how to:

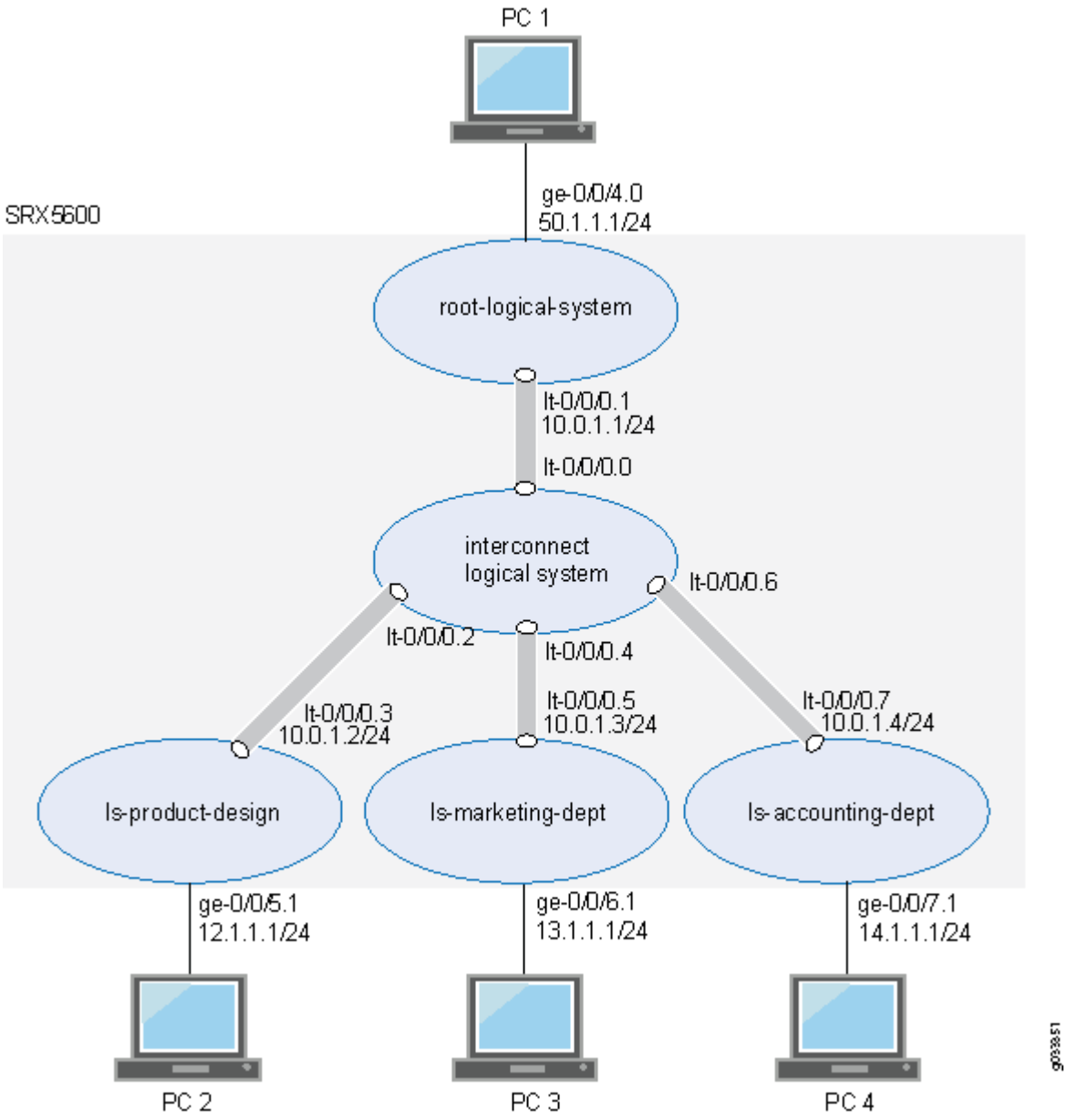
- Create user logical systems and an interconnect logical system that is used as an internal VPLS switch to allow traffic to pass from one logical system to another.
- Create administrators for user logical systems other than the interconnect logical system. A user logical system can have more than one 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.

Topology

Figure 5 on page 56 shows an SRX5600 device deployed and configured for logical systems. The configuration examples reflect this deployment.

Figure 5: SRX Series Firewall Configured for Logical Systems



Configuration

IN THIS SECTION

- Configuring User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System | **57**

Configuring User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System

CLI Quick Configuration

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

```
set 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 "$ABC123"
set system login class ls-design-user logical-system ls-product-design
set system login class ls-design-user permissions view
set system login user lsdesignuser1 full-name lsdesignuser1
set system login user lsdesignuser1 class ls-design-user
set system login user lsdesignuser1 authentication encrypted-password "$ABC123"
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 "$ABC123"
set logical-systems ls-marketing-dept
set system login class ls-marketing-admin logical-system ls-marketing-dept
set system login class ls-marketing-admin permissions all
set system login user lsmarketingadmin1 class ls-marketing-admin
set system login user lsmarketingadmin1 full-name lsmarketingadmin1
set system login user lsmarketingadmin1 authentication encrypted-password "$ABC123"
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 "$ABC123"
set logical-systems ls-accounting-dept
set system login class ls-accounting-admin logical-system ls-accounting-dept
set system login class ls-accounting-admin permissions all
set system login user lsaccountingadmin1 full-name lsaccountingadmin1
set system login user lsaccountingadmin1 class ls-accounting-admin
set system login user lsaccountingadmin1 authentication encrypted-password "$ABC123"
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 CLI User Guide.

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

   #### Step-by-Step Procedure

   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.

Step-by-Step Procedure

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.

   Step-by-Step Procedure

   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.

   Step-by-Step Procedure

   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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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

IN THIS SECTION

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

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

Purpose

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

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 SSH to log in to each user logical system as its user administrator would do.

1. Run SSH specifying the IP address of your SRX Series Firewall.
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 primary logical system at root. Repeat this procedure for all of your user logical systems.

```
login: lsdesignadmin1
Password: Talk1234

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

SEE ALSO

Example: Configuring Logical Systems Security Profiles (Primary Administrators Only) | 74

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only) | 111

RELATED DOCUMENTATION

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding Logical Systems for SRX Series Firewalls | 5

Security Profiles for Logical Systems

IN THIS SECTION

Security profiles for logical systems allow you to allocate resources. Security profiles specifies the number of resources to allocate to a logical system to which the security profile is bound. All system resources are allocated to primary logical system and the primary administrator allocates them to user logical system using security profile. For more information, see the following topics:

Understanding Logical Systems Security Profiles (Primary Administrators Only)

IN THIS SECTION

Logical systems allow you to virtually divide a supported SRX Series Firewall 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 primary 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 Firewall running logical systems can be partitioned into user logical systems, an interconnect logical system, if desired, and the default primary logical system. When the system is initialized, the primary logical system is created at the root level. All system resources are assigned to it, effectively creating a default primary logical system security profile. To distribute security resources across logical systems, the primary 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 primary administrator can configure security profiles and bind them to logical systems. The user logical system administrator configures these resources for his or her 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 primary 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 primary 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 Firewall 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 primary 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 primary 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 primary 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)

  NOTE: IPv6 addresses in IPv6 source pools without PAT are not included in security profiles.

- 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. They 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 primary 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 2 on page 72 shows the security profiles and their zone allocations.

Table 2: 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 primary administrator dynamically increases the reserved zone count specified in this profile.
primary-logical-system-profile • zones maximum quota = 10 • no reserved quota

Table 3 on page 73 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 3: 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 primary-logical-system-profile profile is used exclusively for the primary logical system. • user-logical-system-1 = 4 reserved zones. • user-logical-system-2 = 4 reserved zones. • primary-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. • primary-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 primary-logical-system-profile is bound to the primary logical system and used exclusively for it. • The primary administrator configures a new user logical system called new-user-logical-system and binds security-profile-1 to it.

Table 3: Reserved Resource Allocation Assessment Across Logical Systems *(Continued)*

Reserved Resource Quota Checks Across Logical Systems
Example 3: Fails This configuration is out of bounds: 6+6=12, maximum capacity =10. The primary 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. • primary-logical-system = 0 reserved zones.

SEE ALSO

Example: Configuring Logical Systems Security Profiles (Primary Administrators Only) | **74**

Understanding the Primary Logical Systems and the Primary Administrator Role | **21**

Understanding User Logical Systems and the User Logical System Administrator Role | **50**

Example: Configuring Logical Systems Security Profiles (Primary Administrators Only)

IN THIS SECTION

This example shows how a primary administrator configures three logical system security profiles to assign to user logical systems and the primary 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 Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how this task fits into the overall configuration process.

Overview

IN THIS SECTION

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

- The root-logical-system logical system. The security profile primary-profile is assigned to the primary, 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.

Topology

This configuration relies on the deployment shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set 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 icap-redirect-profile maximum 64
 set system security-profile master-profile icap-redirect-profile reserved 30
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 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 master-profile icap-redirect-profile maximum 64
 set system security-profile master-profile icap-redirect-profile reserved 30
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 master-profile icap-redirect-profile maximum 64
 set system security-profile master-profile icap-redirect-profile reserved 30
 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.

   #### Step-by-Step Procedure

   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 ICAP redirect profiles

   ```
   [edit system security-profile]
   user@host# set master-profile icap-redirect-profile maximum 64 reserved 30
   ```

e. 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
```

f. Enable intrusion detection and prevention (IDP). You can enable IDP only for the primary (root) logical system.

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

g. Bind the security profile to the logical system.

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

2. Create the second security profile.

Step-by-Step Procedure

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 ICAP redirect profiles

```
[edit system security-profile]
user@host# set ls-accnt-mrkt-profile icap-redirect-profile maximum 64 reserved 30
```

e. 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
```

f. 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
```

g. 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.

Step-by-Step Procedure

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 ICAP redirect profiles

```
[edit system security-profile]
user@host# setls-design-profile icap-redirect-profile maximum 64 reserved 30
```

e. 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;
            }
            icap-redirect-profile {
                maximum 64;
                reserved 30;
            }
            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;
            }
            icap-redirect-profile {
                maximum 64;
```

```
                reserved 30;
            }
            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;
            }
            icap-redirect-profile {
                maximum 64;
                reserved 30;
            }
            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;
            }
            icap-redirect-profile {
                maximum 64;
                reserved 30;
            }
            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;
        }
        icap-redirect-profile {
            maximum 64;
            reserved 30;
        }
        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;
        }
        icap-redirect-profile {
            maximum 64;
            reserved 30;
        }
        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

IN THIS SECTION

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

Purpose

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

Action

1. Use SSH to log in to each user logical system as its user logical system administrator.

   Run SSH, specifying the IP address of your SRX Series Firewall.

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
```

SEE ALSO

Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Example: Configuring User Logical Systems Security Profiles

IN THIS SECTION

In this example, you configure the user logical systems security profiles. It provides the information about a resource allocated to the logical system in a security profile.

NOTE:

- SRX4100 and SRX4200 devices support logical system in both transparent and route mode.
- SRX4600 device supports logical system in route mode only.
- Layer 2 cross logical system traffic is not supported.

Requirements

This example uses an SRX4100 and SRX4200 devices running Junos OS with logical systems.

Before you begin:

- Understand the logical system configuration process. See "User Logical Systems Configuration Overview" on page 48 to understand how this task fits into the overall configuration process.

Overview

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

In this example, you configure security features for the user logical system described in Table 4 on page 88. This configuration used by the user logical system administrator to display resource information for a user logical system.

Table 4: Resource Information for a User Logical System

Field Name	Field Description
MAC flags	Status of MAC address learning properties for each interface: • **S**—Static MAC address is configured • **D**—Dynamic MAC address is configured • **L**—Locally learned MAC address is configured • **P**—Persistent static • **C**—Control MAC • **SE**—MAC accounting is enabled • **NM**—Non-configured MAC • **R**—Locally learned MAC address is configured • **O**—Open vSwitch Database (OVSDB) MAC
Ethernet switching table	For learned entries, the time at which the entry was added to the Ethernet switching table.
Logical system	Name of the logical system
Routing instance	Name of the routing instance
VLAN name	Name of the VLAN
MAC address	MAC address or addresses learned on a logical interface
Age	This field is not supported
Logical interface	Name of the logical interface

Table 4: Resource Information for a User Logical System *(Continued)*

Field Name	Field Description
RTR ID	ID of the routing device
NH Index	Software index of the next hop that is used to route the traffic for a given prefix.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set system security-profile security-profile-name logical-system logical-system-name
set logical-systems logical-system-name interfaces xe-0/0/0 unit 0 family ethernet-switching
interface-mode access
set logical-systems logical-system-name interfaces xe-0/0/0 unit 0 family ethernet-switching
vlan members VLAN100
set logical-systems logical-system-name interfaces xe-0/0/1 unit 0 family ethernet-switching
interface-mode access
set logical-systems logical-system-name interfaces xe-0/0/1 unit 0 family ethernet-switching
vlan members VLAN100
set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family ethernet-switching
interface-mode trunk
set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family ethernet-switching
vlan members VLAN200
set logical-systems logical-system-name interfaces xe-0/0/1.0 unit 0 family ethernet-switching
```

```
interface-mode trunk
set logical-systems logical-system-name interfaces xe-0/0/2.0 unit 0 family ethernet-switching
vlan members vlan200
set logical-systems logical-system-name interfaces irb unit 22 family inet address
10.11.11.150/24
set logical-systems logical-system-name security policies default-policy permit-all
set logical-systems logical-system-name security zones security-zone trust host-inbound-traffic
system-services all
set logical-systems logical-system-name security zones security-zone trust host-inbound-traffic
protocols all
set logical-systems logical-system-name security zones security-zone trust interfaces xe-0/0/2.0
set logical-systems logical-system-name security zones security-zone untrust host-inbound-
traffic system-services all
set logical-systems logical-system-name security zones security-zone untrust host-inbound-
traffic protocols all
set logical-systems logical-system-name security zones security-zone untrust interfaces
xe-0/0/2.0
set logical-systems logical-system-name security zones security-zone untrust interfaces
xe-0/0/3.0
set logical-systems logical-system-name vlans VLAN100 vlan-id 100
set logical-systems logical-system-name vlans VLAN100 l3-interface irb.22
```

Procedure

Step-by-Step Procedure

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

To configure user logical systems security profiles:

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

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

2. Configure a security profile and assign it to a logical-system.

```
[edit system security-profile ]
admin@host# set system security-profile security-profile-name logical-system
```

3. Set the interfaces to the appropriate interface modes and specify that the logical interface that will receive the untagged data packets is a member of the native VLAN.

```
[edit logical-systems]
admin@host#set logical-systems logical-system-name interfaces xe-0/0/0 unit 0 family ethernet-switching interface-mode access
admin@host# set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/1 unit 0 family ethernet-switching interface-mode access
admin@host# set logical-systems logical-system-name interfaces xe-0/0/3 unit 0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family ethernet-switching interface-mode trunk
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2 unit 0 family ethernet-switching vlan members VLAN100
admin@host#set logical-systems logical-system-name interfaces xe-0/0/1.0 unit 0 family ethernet-switching interface-mode trunk
admin@host#set logical-systems logical-system-name interfaces xe-0/0/2.0 unit 0 family ethernet-switching vlan members vlan200
```

4. Create the IRB interface and assign it an address in the subnet.

```
[edit interface]
admin@host# set interfaces irb unit 22 family inet address 10.11.11.150/24
```

5. Create the security policy to permit traffic from the trust zone to the untrust zone and assign interfaces to each zone.

```
[edit security policies]
admin@host# set security policies default-policy permit-all
admin@host# set security zones security-zone trust host-inbound-traffic system-services all
admin@host# set security zones security-zone trust host-inbound-traffic protocols all
admin@host# set security zones security-zone trust interfaces xe-0/0/2.0
```

```
admin@host# set security zones security-zone untrust host-inbound-traffic system-services all
admin@host# set security zones security-zone untrust host-inbound-traffic protocols all
admin@host# set security zones security-zone untrust interfaces xe-0/0/2.0
admin@host# set security zones security-zone untrust interfaces xe-0/0/3.0
```

6. Associate an IRB interface with the VLAN.

```
[edit logical-systems]
admin@host# set logical-systems logical-system-name vlans VLAN100 vlan-id 100
admin@host# set logical-systems logical-system-name vlans VLAN100 l3-interface irb.22
```

Results

From configuration mode, confirm your configuration by entering the `show ethernet-switching table` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
admin@host# show ethernet-switching table
ethernet-switching table {
    filter;
    inner-vlan;
    inter-switch-link;
    interface-mode;
    policer;
    recovery-timeout;
    storm-control;
    vlan;
    vlan-auto-sense;
    vlan-rewrite;
}
```

Verification

IN THIS SECTION

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

Verifying User Logical Systems Security Profiles Configuration

Purpose

Verify security policies information.

Action

From operational mode, enter the `show ethernet-switching table` command.

```
admin@host> show ethernet-switching table
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C -
Control MAC
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)


Ethernet switching table : 1 entries, 1 learned
Logical system   : LD2
Routing instance : default
    Vlan                MAC                 MAC         Age    Logical                NH
RTR
    name                address             flags              interface              Index
ID
    VLAN100             d4:04:ff:89:fd:30   D             -    xe-0/0/2.0             0
0
```

Example: Configuring Security log stream for Logical Systems

IN THIS SECTION

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

Requirements

This example uses the SRX Series Firewalls running Junos OS with logical systems.

Before you begin:

- Read "SRX Series Logical Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how this task fits into the overall configuration process.
- See "Example: Configuring Logical Systems Security Profiles (Primary Administrators Only)" on page 74.

Overview

As primary administrator, you can configure a single security profile to assign resources to a specific logical system. Yo can use the same security profile for more than one logical system, or use a mix of both methods. The `set logical-system LSYS1 security log` command is introduced for logging support on SRX Series Firewalls.

Configuration

IN THIS SECTION

Configuring Logical System Security Profiles logical-system

CLI Quick Configuration

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

```
set system security-profile p1 security-log-stream-number reserved 1
set system security-profile p1 security-log-stream-number maximum 2
set system security-profile p1 logical-system LSYS1
```

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 a security profile and specify the number of maximum and reserved policies..

```
[edit system]
user@host# set security-profile p1 security-log-stream-number reserved 1
user@host# set security-profile p1 security-log-stream-number maximum 2
```

2. Assign the configured security profile to LSYS1.

```
user@host# set security-profile p1 logical-system LSYS1
```

Results

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

```
[edit]
user@host# show system security-profile
p1 {
    security-log-stream-number {
        maximum 2;
        reserved 1;
    }
    logical-system LSYS1;
}
```

Verification

IN THIS SECTION

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

Verifying Security Profile Resources for Logical Systems

Purpose

Verify the security resources for each logical system.

Action

From operational mode, enter the `show system security-profile all-resource`, `show system security-profile security-log-stream-number logical-system all`, `show system security-profile security-log-stream-number summary`, or `show system security-profile security-log-stream-number detail logical-system all` command to see the output:

show system security-profile all-resource

```
user@host> show system security-profile all-resource

resource                                usage    reserved     maximum
[logical system name:   root-logical-system]
[security profile name: Default-Profile]
address-book                                0           0         512
auth-entry                                  0           0  2147483647
cpu on CP                               0.00%       1.00%      80.00%
cpu on SPU                              0.00%       1.00%      80.00%
flow-gate                                   0           0      524288
flow-session                                2           0     6291456
nat-cone-binding                            0           0       65536
nat-destination-pool                        0           0        4096
nat-destination-rule                        0           0        8192
nat-nopat-address                           0           0     1048576
nat-pat-address                             0           0        2048
nat-port-ol-ipnumber                        0           0           4
nat-rule-referenced-prefix                  0           0     1048576
nat-source-pool                             0           0        2048
```

```
nat-source-rule                          0          0        8192
nat-static-rule                          0          0       20480
policy                                   0          0       40000
policy-with-count                        0          0        1024
scheduler                                0          0          64
zone                                     0          0         512
```

Meaning

The sample outputs displays information about the resources allocated to the logical system in a security profile. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

Verifying security-log-stream-number for logical-systems

Purpose

Verify the security-log-stream-number for each logical system.

Action

From operational mode, enter the `show system security-profile security-log-stream-number logical-system all` command to see the output:

show system security-profile security-log-stream-number logical-system all

```
user@host> show system security-profile security-log-stream-number logical-system all
logical system name   security profile name       usage    reserved     maximum
root-logical-system   Default-Profile                1           0           3
LSYS1                 sp1                            0           1           3
LSYS2                 sp2                            1           0           3
```

Meaning

The sample output displays the information about a resource allocated to the logical system in a security profile with security profile name. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

Verifying security-log-stream-number summary for logical-systems

Purpose

Verify the security-log-stream-number summary.

Action

From operational mode, enter the `show system security-profile security-log-stream-number summary` command to see the output:

show system security-profile security-log-stream-number summary

```
user@host> show system security-profile security-log-stream-number summary
global used amount      : 0
global maximum quota    : 32
global available amount : 32
total logical systems   : 1
total security profiles : 0
heaviest usage / user   : 0     / root-logical-system
lightest usage / user   : 0     / root-logical-system
```

Meaning

The sample output displays the summary information about the resource for all logical systems.

Verifying security-log-stream-number detail for logical-systems

Purpose

Verify the security-log-stream-number detail.

Action

From operational mode, enter the `show system security-profile security-log-stream-number detail logical-system all` command to see the output:

show system security-profile security-log-stream-number detail logical-system all

```
user@host> show system security-profile security-log-stream-number detail logical-system all
logical system name     : root-logical-system
security profile name   : Default-Profile
used amount             : 0
reserved amount         : 0
maximum quota           : 8
logical system name     : lsys0
security profile name   : lsys_profile
used amount             : 0
reserved amount         : 0
maximum quota           : 8
logical system name     : lsys1
security profile name   : lsys_profile
used amount             : 0
reserved amount         : 0
maximum quota           : 8
logical system name     : lsys2
security profile name   : lsys_profile
used amount             : 0
reserved amount         : 0
maximum quota           : 8
```

Meaning

The sample output displays the detailed level of output for all logical systems.

SEE ALSO

security-profile-resources

CPU Allocation for Logical Systems

IN THIS SECTION

The CPU allocation for logical systems assign the reserved CPU resources to a logical system used to calculate the amount of CPU usage based on the runtime utilization. For more information, see the following topics:

Understanding CPU Allocation and Control

IN THIS SECTION

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 primary administrator can enable CPU resource control and configure CPU utilization parameters for logical systems.

NOTE: Only the primary 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 primary 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 primary administrator are bound to specific logical systems.

When CPU control is enabled, the primary 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 primary 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 primary logical system is 1 percent and the default reserved CPU quota for user logical systems is 0 percent. The primary

administrator can configure reserved CPU quotas even if CPU control is not enabled. The primary administrator can enable or disable CPU control without changing security profiles.

CAUTION: The primary 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 primary 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 primary 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 primary 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: primary 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 103 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?
primary	40%	28.8%	Yes
lsys1	40%	28.8%	Yes
lsys2	40%	14.4%	Yes

CPU Utilization Scenario 2

In this scenario, the primary logical system needs 25 percent of CPU while the two user logical systems need 40 percent. Table 6 on page 103 shows the CPU quota for the primary logical system is equal to the CPU it needs, so no packets are dropped for the primary logical system and CPU control monitors the CPU utilization of the primary logical system. Packets are dropped for lsys1 and lsys2.

Table 6: CPU Utilization Scenario 2

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

CPU Utilization Scenario 3

In this scenario, the primary and lsys2 logical systems need 5 percent and 3 percent of CPU, respectively, while lsys1 needs 40 percent. Table 7 on page 104 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?
primary	5%	5%	No
lsys1	40%	40%	No
lsys2	3%	3%	No

Monitoring CPU Utilization

CPU utilization can be monitored by either the primary administrator or the user logical system administrators. The primary administrator can monitor CPU utilization for the primary 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 primary administrator can view the log file with the `show log lsys-cpu-utilization-log` command.

SEE ALSO

Example: Configuring CPU Utilization (Primary Administrators Only) | 105

Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68

Example: Configuring CPU Utilization (Primary Administrators Only)

IN THIS SECTION

The primary 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

Before you begin:

- Log in to the primary logical system as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.
- Bind security profiles to the primary logical system and user logical systems configured on the device. See "Example: Configuring Logical Systems Security Profiles (Primary Administrators Only)" on page 74.

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 54. The logical systems are bound to the security profiles shown in Table 8 on page 105 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 (primary)	primary-profile	2 percent

Table 8: Logical Systems, Security Profiles, and Reserved CPU Quotas *(Continued)*

Logical System	Security Profile	Reserved CPU Quotas
ls-product-design	ls-design-profile	2 percent
ls-marketing-dept, ls-accounting-dept	ls-accnt-mrkt-profile	1 percent

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set 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 primary logical system as the primary 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

IN THIS SECTION

Confirm that the configuration is working properly.

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%
```

SEE ALSO

Understanding CPU Allocation and Control | **100**

Understanding Logical Systems Security Profiles (Primary Administrators Only) | **68**

Routing and Interfaces for Primary Logical Systems

IN THIS SECTION

Logical systems enables you to configure the interfaces, routing instances and the routing protocol. The primary logical system administrator can display or clear the routing protocol parameters for all logical systems whereas the administrator for the user logical system can display or clear the protocol parameters for their own logical system. For more information, see the following topics:

Understanding Logical Systems Interfaces and Routing Instances

Logical interfaces on the device are allocated among the user logical systems by the primary 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 primary 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, primary, refers to the main inet.0 routing table in the logical system. The primary routing instance is reserved and cannot be specified as a routing instance. Routes are installed in the primary routing instance by default, unless a routing instance is specified. Configure global routing options and protocols for the primary 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 primary 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 primary 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.

SEE ALSO

Example: Configuring Interfaces and Routing Instances for a User Logical Systems | 135

User Logical Systems Configuration Overview | 48

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only)

IN THIS SECTION

This topic covers configuration of interfaces, static routes, and routing instances for the primary 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 Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how and where this procedure fits in the overall primary administrator configuration process.
- Read "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54
- "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 9

Overview

IN THIS SECTION

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.

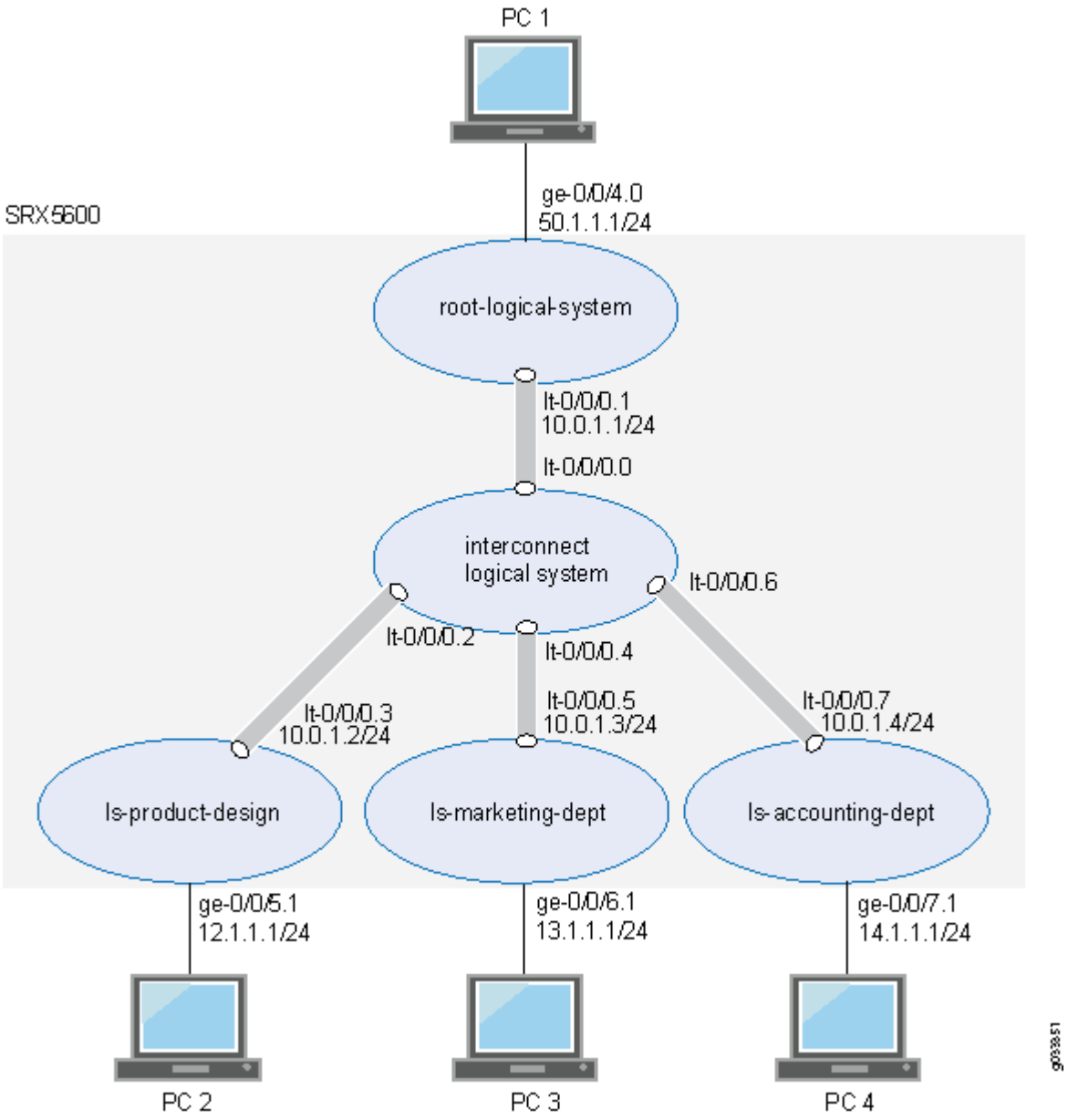
  Because the interconnect logical system acts as a virtual switch, it is configured as a virtual private LAN service (VPLS) routing instance type. The interconnect logical system's lt-0/0/0 interfaces are configured with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the primary 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 primary 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 6 on page 113 shows the topology for this deployment including virtual routers and their interfaces for all logical systems.

Topology

Figure 6: Configuring Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers



Configuration

IN THIS SECTION

This topic explains how to configure interfaces for logical systems.

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System

CLI Quick Configuration

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

```
set 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 Primary Logical System

CLI Quick Configuration

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

```
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 600
set interfaces ge-0/0/4 unit 0 family inet address 50.1.1.1/24
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*.

To configure the primary logical system interfaces:

1. Configure the primary (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 50.1.1.1/24
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 primary 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 50.1.1.1/24;
            }
        }
    }
        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 example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set 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*.

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

IN THIS SECTION

- Verifying That the Static Routes Configured for the Primary Administrator Are Correct | **122**

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

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

Purpose

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

Action

From operational mode, use the `ping` command.

SEE ALSO

- Understanding the Primary Logical Systems and the Primary Administrator Role | **21**
- Understanding User Logical Systems and the User Logical System Administrator Role | **50**
- Understanding the Interconnect Logical System and Logical Tunnel Interfaces | **9**

Example: Configuring OSPF Routing Protocol for the Primary Logical Systems

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the primary logical system as the primary administrator. See "Example: Configuring Root Password for Logical Systems" on page 52.
- Configure logical interfaces ge-0/0/4.0 and lt-0/0/0.1 for the primary logical system and assign them to the vr1-root routing instance. See "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only)" on page 111.

Overview

In this example, you configure OSPF for the primary logical system, called root-logical-system, shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54.

This example enables OSPF routing on the ge-0/0/4.0 and lt-0/0/0.1 interfaces in the primary 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

IN THIS SECTION

- Procedure | 124

Procedure

CLI Quick Configuration

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

```
set 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 primary logical system:

1. Log in to the primary logical system as the primary 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

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying OSPF Interfaces

Purpose

Verify OSPF-enabled interfaces.

Action

From the CLI, enter the `show ospf interface instance 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
```

SEE ALSO

- Understanding Logical Systems Interfaces and Routing Instances | 110
- Example: Configuring OSPF Routing Protocol for a User Logical Systems | 139
- OSPF User Guide

Routing, Interfaces, and NAT for User Logical Systems

IN THIS SECTION

The user logical system enables you to configure routing protocols, interfaces and NAT. Routing protocols handles all routing messages. NAT is a mechanism to translate the IP address of a computer or group of computers into a single public address when the packets are sent out to the internet. For more information, see the following topics:

Understanding Logical Systems 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 configuring NAT in a root system. The primary administrator can configure and monitor NAT in the primary logical system as well as any user logical system.

Starting in Junos OS Release 18.2R1, the NAT functionality is supported for logical systems on SRX4100, and SRX4200 devices in addition to existing support on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

For each user logical system, the primary 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 primary administrator can configure a security profile for the primary logical system that specifies the maximum and reserved numbers of NAT resources applied to the primary logical system. The number of resources configured in the primary 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 primary logical system, the primary administrator can use the same command to view information for the primary logical system, a specific user logical system, or all logical systems.

SEE ALSO

Example: Configuring Network Address Translation for a User Logical Systems | **130**

User Logical Systems Configuration Overview | **48**

Understanding Logical Systems Security Profiles (Primary Administrators Only) | **68**

Introduction to NAT

Example: Configuring Network Address Translation for a User Logical Systems

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical Systems Configuration Overview" on page 48.
- Use the `show system security-profile nat-static-rule` command to see the static NAT resources allocated to the logical system.
- Configure security policies. See "Example: Configuring Security Policies in a User Logical Systems" on page 212.

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 54.

Devices in the ls-product-design-untrust zone access a specific host in the ls-product-design-trust zone by way of the address 12.1.1.200/32. For packets that enter the ls-product-design logical system from the ls-product-design-untrust zone with the destination IP address 12.1.1.200/32, the destination IP address is translated to the 12.1.1.100/32. This example configures the static NAT described in Table 9 on page 131.

Table 9: User Logical System Static NAT Configuration

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

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security 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

IN THIS SECTION

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

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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Network Address Translation | 129

Static NAT Configuration Overview

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

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the user logical system as the user logical system administrator. See "User Logical Systems Configuration Overview" on page 48.
- Determine which logical interfaces and, optionally, which logical tunnel interfaces are allocated to your user logical system by the primary administrator. The primary administrator configures the logical tunnel interfaces. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

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 54.

This example configures the interfaces and routing instances described in Table 10 on page 135.

Table 10: 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

Table 10: User Logical System Interface and Routing Instance Configuration *(Continued)*

Feature	Name	Configuration Parameters

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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set interfaces ge-0/0/5 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 primary 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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Interfaces and Routing Instances | 110

Example: Configuring OSPF Routing Protocol for a User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- 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 Systems" on page 135.

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 54.

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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set 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 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

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying OSPF Interfaces

Purpose

Verify OSPF-enabled interfaces.

Action

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

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

Verifying OSPF Neighbors

Purpose

Verify OSPF neighbors.

Action

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

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

Verifying OSPF Routes

Purpose

Verify OSPF routes.

Action

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

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

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

SEE ALSO

- Understanding Logical Systems Interfaces and Routing Instances | **110**
- Example: Configuring OSPF Routing Protocol for the Primary Logical Systems | **123**
- OSPF User Guide

RELATED DOCUMENTATION

- User Logical Systems Overview | **48**

Security Zones in Logical Systems

IN THIS SECTION

Security zones are the building blocks for policies. Security zones are logical entities to which one or more interfaces are bound and provides a means of distinguishing groups of hosts (user logical systems and other hosts, such as servers), resources from one another in order to apply different security measures. For more information, see the following topics:

Understanding Logical Systems Zones

Security zones are logical entities to which one or more interfaces are bound. Security zones can be configured on the primary logical system by the primary 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 primary 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 primary administrator can configure a security profile for the primary logical system that specifies the maximum and reserved numbers of security zones applied to the primary logical system. The number of zones configured in the primary logical system count toward the maximum number of zones available on the device.

The primary 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 primary logical system or user logical system.

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

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

SEE ALSO

Example: Configuring Security Zones for a User Logical Systems | **163**

User Logical Systems Configuration Overview | **48**

Understanding Logical Systems Security Profiles (Primary Administrators Only) | **68**

Understanding Logical Systems Interfaces and Routing Instances | **110**

Security Zones Overview

Example: Configuring User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- 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 primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

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 54.

This example configures the parameters described in Table 11 on page 147 and Table 12 on page 149.

Table 11: 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

Table 11: ls-marketing-dept Logical System Configuration *(Continued)*

Feature	Name	Configuration Parameters

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

Table 11: ls-marketing-dept Logical System Configuration *(Continued)*

Feature	Name	Configuration Parameters
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 12: 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

Table 12: ls-accounting-dept Logical System Configuration *(Continued)*

Feature	Name	Configuration Parameters

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

Table 12: ls-accounting-dept Logical System Configuration *(Continued)*

Feature	Name	Configuration Parameters
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

IN THIS SECTION

Configuring the ls-marketing-dept User Logical System

CLI Quick Configuration

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

```
set interfaces ge-0/0/6 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
12.12.1.0/24 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 example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces ge-0/0/7 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*.

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

IN THIS SECTION

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

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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Interfaces and Routing Instances | 110

Understanding Logical Systems Zones | 145

Understanding Logical Systems Security Policies | 210

Example: Configuring Security Zones for a User Logical Systems

IN THIS SECTION

Configuration | 165

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 Systems Configuration Overview" on page 48.
- Use the `show system security-profile zones` command to see the zone resources allocated to the logical system.
- Logical interfaces for the user logical system must be configured. See "Example: Configuring Interfaces and Routing Instances for a User Logical Systems" on page 135.

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 54.

This example creates the zones and address books described in Table 13 on page 164.

Table 13: 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

Table 13: User Logical System Zone and Address Book Configuration *(Continued)*

Feature	Name	Configuration Parameters
	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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security address-book 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
```

7.

Results

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

```
lsdesignadmin1@host:ls-product-design# show security
    address-book {
        product-design-internal {
            address product-designers 12.1.1.0/24;
            attach {
                zone ls-product-design-trust;
            }
        }
        product-design-external {
            address marketing 13.1.1.0/24;
            address accounting 14.1.1.0/24;
            address others 12.12.1.0/24;
            address-set otherlsys {
                address marketing;
```

```
                address accounting;
            }
            attach {
                zone ls-product-design-untrust;
            }
        }
    }
        zones {
            security-zone ls-product-design-trust {
                tcp-rst;
                interfaces {
                    ge-0/0/5.1;
                }
            }
            security-zone ls-product-design-untrust {
                interfaces {
                    lt-0/0/0.3;
                }
            }
        }
```

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

SEE ALSO

- Understanding Logical Systems Zones | 145
- User Logical Systems Configuration Overview | 48

RELATED DOCUMENTATION

- Example: Configuring Security Policies in a User Logical Systems | 212

User Authentication for Logical Systems

IN THIS SECTION

User authentication for logical systems enables you to define firewall users and create policies that require the users to authenticate themselves through one of two authentication schemes: pass-through authentication or web authentication. For more information, see the following topics:

Example: Configuring Access Profiles (Primary Administrators Only)

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the primary logical system as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.
- Read *Firewall User Authentication Overview*.

Overview

This example configures an access profile for LDAP authentication for logical system users. This example creates the access profile described in Table 14 on page 170.

NOTE: The primary administrator creates the access profile.

Table 14: 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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

NOTE: You must be logged in as the primary 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 CLI User Guide.

To configure an access profile in the primary logical system:

1. Log in to the primary logical system as the primary 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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Example: Configuring Security Features for the Primary Logical Systems

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the primary logical system as the primary administrator. See "Example: Configuring Root Password for Logical Systems" on page 52.
- Use the `show system security-profile` command to see the resources allocated to the primary logical system.
- Configure logical interfaces for the primary logical system. See "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only)" on page 111.
- Configure the access profile ldap1 in the primary logical system. The ldap1 access profile is used for Web authentication of firewall users.

Overview

In this example, you configure security features for the primary logical system, called root-logical-system, shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54. This example configures the security features described in Table 15 on page 173.

Table 15: 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

Table 15: root-logical-system Security Feature Configuration *(Continued)*

Feature	Name	Configuration Parameter
Address books	root-internal	• Address primaries: 10.12.12.0/24 • Attach to zone ls-root-trust
	root-external	• Address design: 10.12.1.0/24 • Address accounting: 10.14.1.0/24 • Address marketing: 10.13.1.0/24 • 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: primaries • 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: primaries • Application: junos-http, junos-https

Table 15: root-logical-system Security Feature Configuration *(Continued)*

Feature	Name	Configuration Parameter
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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security address-book root-internal address masters 10.12.12.0/24
set security address-book root-internal attach zone ls-root-trust
set security address-book root-external address design 10.12.1.0/24
set security address-book root-external address accounting 10.14.1.0/24
set security address-book root-external address marketing 10.13.1.0/24
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 primary logical system:

1. Log in to the primary logical system as the primary 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 10.12.12.0/24
admin@host# set address-book root-external address design 10.12.1.0/24
admin@host# set address-book root-external address accounting 10.14.1.0/24
admin@host# set address-book root-external address marketing 10.13.1.0/24
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 10.12.12.0/24;
        attach {
            zone ls-root-trust;
        }
    }
    root-external {
        address design 10.12.1.0/24;
        address accounting 10.14.1.0/24;
        address marketing 10.13.1.0/24;
        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

IN THIS SECTION

- Verifying Policy Configuration | 181

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

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.

SEE ALSO

Understanding Logical Systems Zones | 145

Understanding Logical Systems Security Policies | 210

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 primary administrator is responsible for configuring access profiles in the primary 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 primary logical system are available to all user logical systems.

The primary 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 primary administrator uses the `profile` *configuration statement* at the [`edit access`] hierarchy level in the primary 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 primary logical system, the primary administrator can use the same commands to view information for the primary logical system, a specific user logical system, or all logical systems.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68

Firewall User Authentication Overview

Example: Configuring Firewall Authentication for a User Logical System

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- Use the `show system security-profiles auth-entry` command to see the firewall authentication entries allocated to the logical system.
- Access profiles must be configured in the primary logical system by the primary administrator.

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 54.

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 184.

NOTE: This example uses the access profile configured and address book entries configured in "Example: Configuring Security Zones for a User Logical Systems" on page 163.

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 Systems" on page 212.) 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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security policies 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

IN THIS SECTION

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

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
```

SEE ALSO

User Logical Systems Configuration Overview | 48

Example: Configuring Pass-Through Authentication

Understanding Integrated User Firewall support in a Logical System

IN THIS SECTION

Starting in Junos OS Release 18.3R1, the support for authentication sources is extended to include Local authentication, Active Directory (AD) authentication, and firewall authentication in addition to the existing support for authentication sources Juniper Identity Management Service (JIMS) and ClearPass authentication.

Starting in Junos OS Release 18.2R1, the support for user firewall authentication is enhanced using a shared model. In this model, user logical systems share user firewall configuration and authentication entries with the primary logical system and the integrated user firewall authentication is supported in a user logical system.

In the shared model, user firewall related configuration is configured under the primary logical system, such as authentication source, authentication source priority, authentication entries timeout, and IP query or Individual query and so on. The user firewall provides user information service for an application in the SRX Series Firewall, such as policy and logging. Traffic from a user logical system queries authentication tables from the primary logical system.

The authentication tables are managed by a primary logical system. The user logical systems share the authentication tables. Traffic from the primary logical system and the user logical systems query the same authentication table. User logical systems enable the use of the source-identity in security policy.

For example, if the primary logical system is configured with **employee** and the user logical system is configured with the source-identity **manager**, then the reference group of this authentication entry includes **employee** and **manager**. This reference group contains the same authentication entries from primary logical system and user logical system.

Starting in Junos OS Release 19.3R1, support for user firewall authentication is enhanced by using a customized model through integrated JIMS with active mode. In this model, the logical system extracts the authentication entries from the root level. The primary logical system is configured to the JIMS server based on the logical system and tenant system name. In active mode the SRX Series Firewall actively queries the authenticaton entries received from the JIMS server through HTTPs protocol. To reduce the data exchange, firewall filters are applied.

The user firewall uses the logical system name as a differentiator and is consistent between the JIMS server and SRX Series Firewall. The JIMS server sends the differentiator which is included in the

authentication entry. The authentication entries are distributed into the root logical system, when the differentiator is set as default for primary logical system.

The user firewall supports In-service software upgrade (ISSU) for logical systems, as user firewall changes the internal database table format from Junos OS Release 19.2R1 onwards. Prior to Junos OS Release 19.2R1, ISSU is not supported for logical systems.

Limitation of Using User Firewall Authentication

Using user firewall authentication on tenant systems has the following limitation:

- The authentication entries are collected by the JIMS server based on the IP address from the customer network. If the IP addresses overlap, then the authentication entry changes when users log in under different user logical systems.

Limitation of Using User Firewall Authentication in Customized Model on Logical Systems

Using user firewall authentication in customized model on logical systems has the following limitation:

- The JIMS server configurations to be configured under the root logical systems.
- The logical system name should be consistent and unique between the JIMS server and the SRX Series Firewall.

SEE ALSO

show services user-identification authentication-table

Example: Configuring Integrated User Firewall Identification Management for a User Logical System

IN THIS SECTION

This example shows how to configure the SRX Series Firewall's advanced query feature for obtaining user identity information from the Juniper Identity Management Service (JIMS) and the security policy to match the source identity for a user logical system. In the root logical system, user firewall is configured with JIMS, and then the root logical system manages all of authentication entries coming from JIMS. In this example, all of user logical systems share their authentication entries with the root logical system.

Requirements

This example uses the following hardware and software components:

- SRX1500 devices operating in chassis clustering
- JIMS server
- Junos OS Release 18.2 R1

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical Systems Overview" on page 48
- Configure user logical systems lsys1 and lsys2. See Example: Configuring User Logical Systems
- Configure security profile on primary logical system and assign it to user logical systems lsys1 and lsys2. See Example: Configuring Logical Systems Security Profiles (Primary Administrators Only)
- Configure interfaces and routing options on logical systems root logical system, user logical systems lsys1, and lsys2. See Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only) and Example: Configuring Interfaces and Routing Instances for a User Logical Systems
- Configure security policies for a user logical systems. See Example: Configuring Security Policies in a User Logical Systems
- Configure zones for a user logical system. See Example: Configuring Security Zones for a User Logical Systems
- Configure logical systems in a basic active/passive chassis cluster. See Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Primary Administrators Only)

Overview

In this example, you can configure JIMS with HTTPs connection on port 443 and primary server with IPv4 address on primary logical system, policy p1 with source-identity "group1" of dc0 domain on logical system lsys1, policy p1 with source-identity "group1" of dc0 domain on logical system lsys2, and send traffic from and through logical system lsys1 to logical system lsys2. You can view the authentication entries on primary logical system and user logical systems (lsys1 and lsys2) even after rebooting the primary node.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 match destination-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 match application any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 then permit
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 match source-identity "example.com\group1"
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_trust policy
lsys1_policy1 then permit
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust policy
lsys1_policy2 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust policy
lsys1_policy2 match destination-address any
```

```
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust policy
lsys1_policy2 match application any
set logical-systems lsys1 security policies from-zone lsys1_trust to-zone lsys1_untrust policy
lsys1_policy2 then permit
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust policy
lsys1_policy3 match source-address any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust policy
lsys1_policy3 match destination-address any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust policy
lsys1_policy3 match application any
set logical-systems lsys1 security policies from-zone lsys1_untrust to-zone lsys1_trust policy
lsys1_policy3 then permit
set logical-systems lsys1 security policies policy-rematch
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust policy
lsys2_policy1 match source-address any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust policy
lsys2_policy1 match destination-address any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust policy
lsys2_policy1 match application any
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust policy
lsys2_policy1 match source-identity "example.com\group2"
set logical-systems lsys2 security policies from-zone lsys2_untrust to-zone lsys2_untrust policy
lsys2_policy1 then permit
set logical-systems lsys2 security policies policy-rematch
set services user-identification identity-management connection connect-method https
set services user-identification identity-management connection port 443
set services user-identification identity-management connection primary address 192.0.2.5
set services user-identification identity-management connection primary client-id otest
set services user-identification identity-management connection primary client-secret "$ABC123"
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match source-
address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
destination-address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
application any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 then permit
set security policies policy-rematch
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic system-
services all
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic protocols all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic system-
services all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic protocols
```

```
all
set firewall family inet filter impair-ldap term allow_all then accept
```

Configuring user firewall identification management

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 user firewall identification management:

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

```
user@host> configure
user@host#
```

2. Create logical systems.

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

3. Configure a security policy lsys1_policy1 with source-identity group1 on logical system lsys1 that permits traffic from lsys1_trust to lsys1_trust.

```
[edit security policies]
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match source-
address any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
destination-address any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match
application any
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 match source-
identity "example.com\group1"
user@host#set from-zone lsys1_trust to-zone lsys1_trust policy lsys1_policy1 then permit
```

4. Configure a security policy lsys1_policy2 that permits traffic from lsys1_trust to lsys1_untrust.

```
[edit security policies]
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2 match source-address any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2 match destination-address any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2 match application any
user@host#set from-zone lsys1_trust to-zone lsys1_untrust policy lsys1_policy2 then permit
```

5. Configure a security policy lsys1_policy3 that permits traffic from lsys1_untrust to lsys1_trust.

```
[edit security policies]
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3 match source-address any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3 match destination-address any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3 match application any
user@host#set from-zone lsys1_untrust to-zone lsys1_trust policy lsys1_policy3 then permit
user@host#set policy-rematch
```

6. Configure security zone and assign interfaces to each zone.

```
[edit security zones]
user@host#set security-zone lsys1_trust interfaces reth2.0 host-inbound-traffic system-services all
user@host#set security-zone lsys1_trust interfaces reth2.0 host-inbound-traffic protocols all
user@host#set security-zone lsys1_trust interfaces lt-0/0/0.11 host-inbound-traffic system-services all
user@host#set security-zone lsys1_trust interfaces lt-0/0/0.11 host-inbound-traffic protocols all
user@host#set security-zone lsys1_untrust interfaces reth3.0 host-inbound-traffic system-services all
user@host#set security-zone lsys1_untrust interfaces reth3.0 host-inbound-traffic protocols all
```

7. Configure a security policy lsys2_policy1 with source-identity group1 that permits traffic from lsys2_untrust to lsys2_untrust on lsys2.

```
[edit security policies]
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1 match
source-address any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1 match
destination-address any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1 match
application any
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1 match
source-identity "example.com\group2"
user@host#set from-zone lsys2_untrust to-zone lsys2_untrust policy lsys2_policy1 then permit
user@host#set policy-rematch
```

8. Configure security zones and assign interfaces to each zone on lsys2.

```
[edit security zones]
user@host#set security-zone lsys2_untrust interfaces reth4.0 host-inbound-traffic system-
services all
user@host#set security-zone lsys2_untrust interfaces reth4.0 host-inbound-traffic protocols
all
user@host#set security-zone lsys2_untrust interfaces lt-0/0/0.21 host-inbound-traffic
system-services all
user@host#set security-zone lsys2_untrust interfaces lt-0/0/0.21 host-inbound-traffic
protocols all
```

9. Configure JIMS as the authentication source for advanced query requests with the primary address. The SRX Series Firewall requires this information to contact the server.

```
[edit services user-identification identity-management]
user@host#set connection port 443
user@host#set connection connect-method https
user@host#set connection primary address 192.0.2.5
user@host#set connection primary client-id otest
user@host#set connection primary client-secret test
user@host#set authentication-entry-timeout 0
```

10. Configure security policies and zones on primary logical system.

```
[edit security policies]
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match source-
address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match destination-
address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match application
any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 then permit
user@host#set policy-rematch
```

11. Configure security zones and assign interfaces to each zone on primary logical system.

```
[edit security zones]
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic system-
services all
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic protocols all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic system-
services all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic protocols
all
user@host#set firewall family inet filter impair-ldap term allow_all then accept
```

Results

From configuration mode, confirm your configuration by entering the `show services user-identification identity-management` `show chassis cluster` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show services user-identification identity-management
connection {
    connect-method https;
    port 443;
    primary {
        address 192.0.2.5;
        client-id otest;
        client-secret "$ABC123"; ## SECRET-DATA
```

```
    }
}
```

```
user@host# show chassis cluster
reth-count 5;
    control-ports {
    fpc 3 port 0;
    fpc 9 port 0;
}
redundancy-group 0 {
    node 0 priority 200;
    node 1 priority 1;
}
redundancy-group 1 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 2 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 3 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 4 {
    node 0 priority 100;
    node 1 priority 1;
}
```

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

Verification

IN THIS SECTION

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

Verifying chassis cluster status and authentication entries

Purpose

To verify authentication entries in a logical system.

Action

To verify the configuration is working properly, enter the `show services user-identification authentication-table authentication-source identity-management logical-system all` command.

```
user@host> show services user-identification authentication-table authentication-source identity-
management logical-system all
node0:
--------------------------------------------------------------------------
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP       Username       groups(Ref by policy)          state
2001:db8:aaaa:  N/A                                           Valid
2001:db8:aaaa:  administrator                                 Valid
203.0.113.50    administrator                                 Valid
node1:
--------------------------------------------------------------------------
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP       Username       groups(Ref by policy)          state
2001:db8:aaaa:  N/A                                           Valid
2001:db8:aaaa:  administrator                                 Valid
203.0.113.50    administrator                                 Valid
```

Meaning

The output displays the authentication entries that are shared from user logical system to root logical system.

Verifying chassis cluster status

Purpose

Verify chassis cluster status after rebooting the primary node.

Action

To verify the configuration is working properly, enter the `show chassis cluster status` command.

```
user@host> show chassis cluster status
Monitor Failure codes:
CS  Cold Sync monitoring        FL  Fabric Connection monitoring
GR  GRES monitoring             HW  Hardware monitoring
IF  Interface monitoring        IP  IP monitoring
LB  Loopback monitoring         MB  Mbuf monitoring
NH  Nexthop monitoring          NP  NPC monitoring
SP  SPU monitoring              SM  Schedule monitoring
CF  Config Sync monitoring      RE  Relinquish monitoring
Cluster ID: 6
Node   Priority Status               Preempt Manual   Monitor-failures
Redundancy group: 0 , Failover count: 0
node0  200      hold                 no      no       None
node1  1        secondary            no      no       None
Redundancy group: 1 , Failover count: 0
node0  0        hold                 no      no       CS
node1  1        secondary            no      no       None
Redundancy group: 2 , Failover count: 0
node0  0        hold                 no      no       CS
node1  1        secondary            no      no       None
Redundancy group: 3 , Failover count: 0
node0  0        hold                 no      no       CS
node1  1        secondary            no      no       None
Redundancy group: 4 , Failover count: 0
node0  0        hold                 no      no       CS
node1  1        secondary            no      no       None
```

Meaning

The output displays user identification management session existing on lsys1 and lsys2 after rebooting the primary node.

SEE ALSO

show services user-identification authentication-table

Example: Configure Integrated User Firewall in Customized Model for Logical System

IN THIS SECTION

This example shows how to configure the integrated user firewall by using a customized model through the Juniper Identity Management Service (JIMS) server with active mode for a logical system. The primary logical systems does not share the authentication entries with the logical system. The SRX Series Firewall queries the authentication entries received from the JIMS server through HTTPs protocol in active mode.

In this example following configurations are performed:

- Active JIMS Server Configuration
- Logical System IP Query Configuration
- Logical System Authentication Entry Configuration
- Logical System Security Policy Configuration

Requirements

This example uses the following hardware and software components:

- JIMS server version 2.0
- Junos OS Release 19.3R1

Before you begin, be sure you have following information:

- The IP address of the JIMS server.
- The port number on the JIMS server for receiving HTTPs requests.
- The client ID from the JIMS server for active query server.
- The client secret from the JIMS server for active query server.

Overview

In this example, you can configure JIMS with HTTPs connection on port 443 and primary server with IPv4 address on the primary logical system, policy p2 with source-identity `group1` on logical system `LSYS1`.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set services user-identification logical-domain-identity-management active query-server jims1
connection connect-method https
set services user-identification logical-domain-identity-management active query-server jims1
connection port 443
set services user-identification logical-domain-identity-management active query-server jims1
connection primary address 192.0.2.5
set services user-identification logical-domain-identity-management active query-server jims1
connection primary client-id otest
set services user-identification logical-domain-identity-management active query-server jims1
connection primary client-secret "$ABC123"
set logical-systems LSYS1 services user-identification logical-domain-identity-management active
ip-query query-delay-time 30
set logical-systems LSYS1 services user-identification logical-domain-identity-management active
```

```
invalid-authentication-entry-timeout 1
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy p2 match
source-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy p2 match
destination-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy p2 match
application any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy p2 match
source-identity "example.com\group1"
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy p2 then permit
```

Configuring Integrated User Firewall in Customized Model:

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 configuring Integrated User Firewall in Customized Model:

1. Configure JIMS as the authentication source for advanced query requests with the primary address. The SRX Series Firewall requires this information to contact the server.

```
user@host# set services user-identification logical-domain-identity-management active query-
server jims1 connection connect-method https
user@host# set services user-identification logical-domain-identity-management active query-
server jims1 connection port 443
user@host# set services user-identification logical-domain-identity-management active query-
server jims1 connection primary address 192.0.2.5
user@host# set services user-identification logical-domain-identity-management active query-
server jims1 connection primary client-id otest
user@host# set services user-identification logical-domain-identity-management active query-
server jims1 connection primary client-secret "$ABC123"
```

2. Configure the IP query delay time for LSYS1.

```
user@host# set logical-systems LSYS1 services user-identification logical-domain-identity-
management active ip-query query-delay-time 30
```

3. Configure the authentication entry attributes for LSYS1.

```
user@host# set logical-systems LSYS1 services user-identification logical-domain-identity-
management active invalid-authentication-entry-timeout 1
```

4. Configure the security policy p2 that permits traffic from-zone untrust to-zone trust for LSYS1.

```
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
p2 match source-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
p2 match destination-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
p2 match application any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
p2 match source-identity "example.com\group1"
user@host#set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
p2 then permit
```

Results

From configuration mode, confirm your configuration by entering the `show services user-identification logical-domain-identity-management` and `show logical-systems LSYS1` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show services user-identification logical-domain-identity-management
active {
    query-server jims1 {
        connection {
            connect-method https;
            port 443;
            primary {
                address 192.0.2.5;
                client-id otest;
                client-secret "$ABC123"; ## SECRET-DATA
            }
        }
```

```
    }
}
```

```
user@host# show logical-systems LSYS1
security {
    policies {
        from-zone untrust to-zone trust {
            policy p2 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                    source-identity "example.com\group1";
                }
                then {
                    permit;
                }
            }
        }
    }
}
services {
    user-identification {
        logical-domain-identity-management {
            active {
                invalid-authentication-entry-timeout 1;
                ip-query {
                    query-delay-time 30;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying the User Identification Identity Management status

Purpose

Verify the user identification status for identity-management as the authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification logical-domain-identity-management status` command.

```
user@host> show services user-identification logical-domain-identity-management status
node0:
--------------------------------------------------------------------------
      Query server name                :jims1
      Primary server :
     Address                      : 192.0.2.5
     Port                         : 443
     Connection method            : HTTPS
     Connection status            : Online
     Last received status message : OK (200)
     Access token                 : isdHIbl8BXwxFftMRubGVsELRukYXtW3rtKmHiL
     Token expire time            : 2017-11-27 23:45:22
     Secondary server :
     Address                      : Not configured
```

Meaning

The output displays the statistical data about the advanced user query function batch queries and IP queries, or show status on the Juniper Identity Management Service servers.

Verifying the User Identification Identity Management status counters

Purpose

Verify the user identification counters for identity-management as the authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification logical-domain-identity-management counters` command.

```
user@host> show services user-identification logical-domain-identity-management counters
node0:
      --------------------------------------------------------------------------
   Query server name                      :jims1
    Primary server :
     Address                           : 192.0.2.5
     Batch query sent number           : 65381
     Batch query total response number : 64930
     Batch query error response number : 38
     Batch query last response time    : 2018-08-14 15:10:52
     IP query sent number              : 10
     IP query total response number    : 10
     IP query error response number    : 0
     IP query last response time       : 2018-08-13 12:41:56
  Secondary server :
 Address                           : Not configured
```

Meaning

The output displays the statistical data about the advanced user query function batch queries and IP queries, or show counters on the Juniper Identity Management Service servers.

Verifying the User Identification Authentication Table

Purpose

Verify the user identity information authentication table entries for the specified authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification authentication-table authentication-source all logical-system LSYS1` command.

```
user@host> show services user-identification authentication-table authentication-source all
logical-system LSYS1
node0:
      --------------------------------------------------------------------------
   Logical System: LSYS1
Domain: example.com
Total entries: 4
Source IP           Username       groups(Ref by policy)          state
10.12.0.2         administrator  posture-healthy               Valid
10.12.0.15        administrator  posture-healthy               Valid
2001:db8::5         N/A            posture-healthy                Valid
2001:db8::342c:302b N/A            posture-healthy                Valid
```

Meaning

The output displays the entire content of the specified authentication source's authentication table, or a specific domain, group, or user based on the user name. Display the identity information for a user based on the IP address of the user's device.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.3R1	Starting in Junos OS Release 19.3R1, support for user firewall authentication is enhanced by using a customized model through integrated JIMS with active mode.

18.3R1	Starting in Junos OS Release 18.3R1, the support for authentication sources is extended to include Local authentication, Active Directory (AD) authentication, and firewall authentication in addition to the existing support for authentication sources Juniper Identity Management Service (JIMS) and ClearPass authentication.
18.2R1	Starting in Junos OS Release 18.2R1, the support for user firewall authentication is enhanced using a shared model. In this model, user logical systems share user firewall configuration and authentication entries with the primary logical system and the integrated user firewall authentication is supported in a user logical system.

RELATED DOCUMENTATION

Example: Configuring Security log stream for Logical Systems | 93

Security Policies for Logical Systems

IN THIS SECTION

Security policies are used to secure business and control access to LAN resources. Secure access is required both within the company across the LAN and in its interactions with external networks such as the Internet. Junos OS provides powerful network security features through its stateful firewall, application firewall, and user identity firewall. All three types of firewall enforcement are implemented through security policies. For more information, see the following topics:

Understanding Logical Systems Security Policies

IN THIS SECTION

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 primary 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 primary administrator.

Starting in Junos OS Release 18.4R1, the user can create dynamic address within a logical system. A dynamic address entry contains IP addresses and prefixes extracted from external sources. The security policies use the dynamic address in the source-address field or destination-address field.

A dynamic address entry (DAE) is a group of IP addresses that can be entered manually or imported from external sources within logical systems. The DAE feature allows feed-based IP objects to be used in security policies to either deny or allow traffic based on either source or destination IP criteria.

NOTE: The maximum number of DAE depends on the dynamic-addresses assigned to the logical systems. Starting in Junos 18.4R1, the `set security dynamic-address feed-server` command can be configured under the logical systems.

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

SEE ALSO

Example: Configuring Security Policies in a User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- Use the `show system security-profiles policy` command to see the security policy resources allocated to the logical system.
- Configure zones and address books. See "Example: Configuring Security Zones for a User Logical Systems" on page 163.

Overview

IN THIS SECTION

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 54.

This example configures the security policies described in Table 17 on page 213.

Table 17: 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

Topology

Configuration

IN THIS SECTION

- Procedure | 214

Procedure

CLI Quick Configuration

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

```
set security policies 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

IN THIS SECTION

- Verifying Policy Configuration | 216

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

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.

SEE ALSO

Understanding Logical Systems Security Policies | 210

User Logical Systems Configuration Overview | 48

Troubleshooting Security Policies

Configuring Dynamic Address for Logical Systems

A dynamic address entry in logical systems provides dynamic IP address information to security policies. To use dynamic address, you must specify basic information of dynamic address including their names, feeds and properties for a logical system.

- Read the Example: Configuring Security Policies in a User Logical Systems to understand how and where this procedure fits to configure the security policy.

To configure dynamic address in IPv4 networks within a logical system:

1. Define the logical system name as LSYS1.

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

2. Create dynamic address within a logical system.

```
[edit logical-systems LSYS1]
user@host# set security dynamic-address address-name Ipv4 profile category IPFilter feed fd1
```

3. Confirm your configuration by entering the `show logical-systems LSYS1 security dynamic-address` command.

```
[edit]
user@host# show logical-systems LSYS1 security dynamic-address
address-name Ipv4 {
    profile {
```

```
        category GeoIP;
        category IPFilter {
            feed fd1;
            }
        }
    }
}
```

- To configure the security policies in the logical system:

  1. Define the logical system name as LSYS1.

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

  2. Create a security policy as p1 that permits traffic from zone trust to zone untrust and configure the match condition.

     ```
     [edit logical-systems LSYS1 security policies from-zone trust to-zone untrust]
     user@host# set policy p1 match source-address any
     user@host# set policy p1 match destination-address any
     user@host# set policy p1 match application any
     user@host# set policy p1 then permit
     ```

  3. Confirm your configuration by entering the `show logical-systems LSYS1 security policies` command.

     ```
     [edit]
     user@host# show logical-systems LSYS1 security policies
     from-zone trust to-zone untrust {
         policy p1 {
             match {
                 source-address any;
                 destination-address any;
                 application any;
             }
             then {
                 permit;
             }
     ```

```
    }
}
```

Screen Options for User Logical Systems

IN THIS SECTION

Screen options on SRX Series Firewalls prevent attacks, such as IP address sweeps, port scans, denial of service (DOS) attacks, ICMP, UDP, and SYN floods. For more information, see the following topics:

Understanding Logical Systems 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 primary administrator can configure screen options for the primary 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 primary administrator.

SEE ALSO

Example: Configuring Screen Options for a User Logical Systems | 220

User Logical Systems Configuration Overview | 48

Attack Detection and Prevention Overview

Example: Configuring Screen Options for a User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- Configure zones for the user logical system. See "Example: Configuring Security Zones for a User Logical Systems" on page 163.

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 54.

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 18 on page 220.

Table 18: 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

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security 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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Screen Options | 219

RELATED DOCUMENTATION

IDP for Logical Systems | 269

Secure Wire for Logical Systems

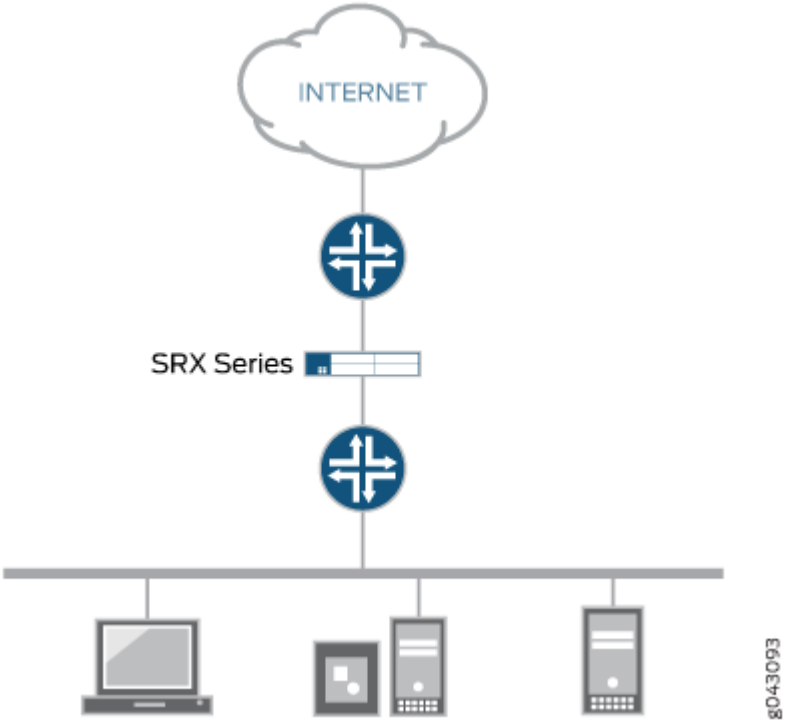
IN THIS SECTION

Secure Wire for Logical Systems Overview

IN THIS SECTION

You can forward the traffic that arrives on a specific interface without any change through another interface on logical systems. This mapping of interfaces on logical systems is called secure wire. Secure wire allows an SRX Series Firewall to deploy in the path of network traffic without changing the routing tables or a reconfiguration of neighboring devices. Figure 7 on page 224 shows a typical in-path deployment of an SRX Series Firewall with secure wire.

Figure 7: SRX Series Firewall In-Path Deployment with Secure Wire



Secure wire maps two peer interfaces. It differs from transparent and route modes, and there is no switching or routing lookup to forward traffic. When security policy permits the traffic, secure wire forwards a packet arriving on one peer interface immediately to the other peer interface without change. There is no routing or switching decision made on the packet. Secure wire also forwards the return traffic unchanged. The secure wire feature is supported for both IPv4 and IPv6 traffic on Ethernet logical interfaces only.

Secure wire is a special case of Layer 2 transparent mode on SRX Series Firewalls that provide point-to-point connections. This means that the two interfaces of a secure wire must directly connect to Layer 3 entities, such as routers or hosts. You can connect secure wire interfaces to switches. However, note that when security policy permits traffic, a secure wire interface forwards all arriving traffic to the peer interface.

Secure wire can coexist with Layer 3 mode. While you configure Layer 2 and Layer 3 interfaces at the same time, traffic forwarding occurs independently on Layer 2 and Layer 3 interfaces.

Secure wire can coexist with Layer 2 transparent mode. If both features exist on the same SRX Series Firewall, you need to configure them in different VLANs.

Secure wire support for root logical system extends to user logical systems. You can forward traffic immediately that arrives on a specific interface to another interface without modifying any received frames on the user logical systems.

Limitations

Secure wire doesn't support:

- IRB interface
- Z-mode
- MPLS label encapsulation
- Tenant system
- Interconnect logical system

Example: Configure Secure Wire for User Logical Systems

IN THIS SECTION

In this example, you can configure secure wire for a user logical system and forward traffic from one interface to another interface without changing any frame.

Requirements

Before you begin:

- Configure security profile for a user logical system, see "Example: Configuring User Logical Systems Security Profiles" on page 86.

Overview

In this example, you can configure 10-Gigabit Ethernet interfaces xe-1/0/1 and xe-1/0/2 under a user logical system, called LSYS1. You can configure secure wire resource allocation per logical system. When traffic passes to xe-1/0/1 interface, without changing any frame, secure wire forwards the traffic to xe-1/0/2 interface based on the defined security policy.

Configuration

IN THIS SECTION

Procedure

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.

```
user@host#set logical-systems LSYS1 security forwarding-options secure-wire myLSYS1sw01
interface xe-1/0/1.0
user@host#set logical-systems LSYS1 security forwarding-options secure-wire myLSYS1sw01
interface xe-1/0/2.0
user@host#set system security-profile prof1 secure-wire maximum 100
user@host#set system security-profile prof1 secure-wire 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 CLI User Guide.

1. Configure secure wire under a user logical system.

```
[edit]
user@host#set logical-systems LSYS1 security forwarding-options secure-wire myLSYS1sw01
```

```
interface xe-1/0/1.0
user@host#set logical-systems LSYS1 security forwarding-options secure-wire myLSYS1sw01
interface xe-1/0/2.0
```

2. Create the security profile, and specify the number of maximum and reserved quota.

```
[edit]
user@host#set system security-profile prof1 secure-wire maximum 100
user@host#set system security-profile prof1 secure-wire reserved 1
```

Results

From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1 security forwarding-options secure-wire myLSYS1sw01`, and `show system security-profile prof1` 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 security forwarding-options secure-wire myLSYS1sw01
interface [ xe-1/0/1.0 xe-1/0/2.0 ];
```

```
user@host#show system security-profile prof1
    secure-wire {
        maximum 100;
        reserved 1;
    }
    logical-system LSYS1;
```

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify Secure Wire Mapping

Purpose

Verify the secure wire mapping.

Action

From operational mode, enter the `show security forward-options secure-wire logical-system LSYS1` command.

```
Logical System       Secure wire                    Interface       Link  Interface       Link

LSYS1                myLSYS1sw01                    xe-1/0/1.0      up    xe-1/0/2.0      up
Total secure wires: 1
```

Verify Resource Allocation

Purpose

Verify the resource allocation for a user logical system.

Action

From operational mode, enter the `show system security-profile secure-wire logical-system LSYS1` command.

```
logical-system tenant name   security profile name       usage    reserved     maximum

LSYS1                        prof1                           1           1         100
```

RELATED DOCUMENTATION

- *security-profile*
- secure-wire

show security forward-options secure-wire

show system security-profile secure-wire

VPNs in Logical Systems

IN THIS SECTION

A VPN is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. VPN prevents unauthorized access eavesdropping on the traffic, and allows the user to conduct work remotely. For more information, see the following topics:

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 primary administrator.

NOTE: The external interface configured under the gateway configuration can only be a part of the root logical system.

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

In addition to configuring IKE and IPsec SAs for each VPN, the primary 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.

NOTE: Traffic selectors are not supported in logical systems.

The primary 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 primary logical system. For the primary logical system, the primary 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 primary administrator in the primary logical system. For the VPN monitor source interface, the primary administrator must specify the st0 interface; a physical interface for a user logical system cannot be specified.

SEE ALSO

Understanding Route-Based IPsec VPNs

User Logical Systems Configuration Overview | 48

Example: Configuring IKE and IPsec SAs for a VPN Tunnel (Primary Administrators Only) | 231

Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems | 241

Example: Configuring IKE and IPsec SAs for a VPN Tunnel (Primary Administrators Only)

IN THIS SECTION

The primary 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 primary logical system as the primary administrator. See "'Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.
- Read *Understanding Route-Based IPsec VPNs*.

Overview

IN THIS SECTION

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 19 on page 232.

Table 19: 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
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

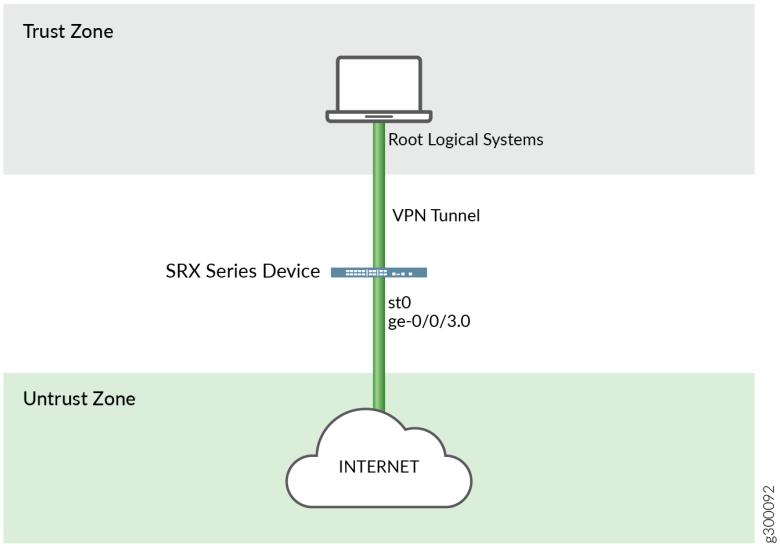
Table 19: Logical System VPN Tunnel Configuration *(Continued)*

Feature	Name	Configuration Parameters
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

Topology

Figure 8 on page 233 shows the topology for logical systems VPN tunnel.

Figure 8: Logical systems VPN tunnel



Configuration

IN THIS SECTION

- Procedure | 234

Procedure

CLI Quick Configuration

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

```
set 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 "$ABC123"
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 primary logical system as the primary 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 "$ABC123"; ## 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

IN THIS SECTION

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

Verifying the IKE on Logical System

Purpose

Verify that the IKE support on Logical Systems.

Action

From operational mode, enter the `show security ike sa detail` command.

```
user@host> show security ike sa detail
IKE peer 2.2.2.2, Index 7796166, Gateway Name: GW1
  Role: Initiator, State: UP
  Initiator cookie: a1a6b1516bc43d54, Responder cookie: f0846e4239c817f8
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 3.3.3.2:500, Remote: 2.2.2.2:500
  Lifetime: Expires in 3585 seconds
  Reauth Lifetime: Disabled
  IKE Fragmentation: Disabled, Size: 0
  Remote Access Client Info: Unknown Client
  Peer ike-id: 2.2.2.2
  AAA assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha256-128
```

```
   Encryption            : aes256-cbc
   Pseudo random function: hmac-sha256
   Diffie-Hellman group  : DH-group-14
  Traffic statistics:
   Input  bytes  :                1056
   Output bytes  :                1311
   Input  packets:                   2
   Output packets:                   4
   Input  fragmentated packets:      0
   Output fragmentated packets:      0
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Initiator, Message ID: 0
    Local: 3.3.3.2:500, Remote: 2.2.2.2:500
    Local identity: r0r2_store1@juniper.net
    Remote identity: 2.2.2.2
    Flags: IKE SA is created
```

Meaning

The output displays summary information about ike details.

Verifying the IPsec on Logical System

Purpose

Verify that the IPsec SA support on Logical Systems.

Action

From operational mode, enter the `show security ipsec sa detail` command.

```
user@host> show security ipsec sa detail
ID: 67109793 Virtual-system: root, VPN Name: VPN1
  Local Gateway: 3.3.3.2, Remote Gateway: 2.2.2.2
  Traffic Selector Name: VPN1_TS1
  Local Identity: ipv4(51.0.1.0-51.0.1.255)
  Remote Identity: ipv4(41.0.1.0-41.0.1.255)
  Version: IKEv1
  DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1
```

```
  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x2c608b29
  Tunnel events:
    Wed Aug 16 2017 23:50:07 -0700: IPSec SA negotiation successfully completed (1 times)
    Wed Aug 16 2017 23:50:07 -0700: IKE SA negotiation successfully completed (1 times)
    Wed Aug 16 2017 23:49:46 -0700: Negotiation failed with error code AUTHENTICATION_FAILED
received from peer (2 times)
    Wed Aug 16 2017 23:49:30 -0700: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Direction: inbound, SPI: e651d79e, AUX-SPI: 0, VPN Monitoring: -
    Hard lifetime: Expires in 2552 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 1988 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
  Direction: outbound, SPI: 8ac9ce8, AUX-SPI: 0, VPN Monitoring: -
    Hard lifetime: Expires in 2552 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 1988 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

Meaning

The output displays summary information about ipsec details.

SEE ALSO

Example: Configuring a Route-Based VPN Tunnel in a User Logical Systems | 241

Understanding Route-Based VPN Tunnels in Logical Systems | 229

User Logical Systems Configuration Overview | 48

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

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- 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 primary administrator. See "Example: Configuring IKE and IPsec SAs for a VPN Tunnel (Primary Administrators Only)" on page 231.

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 54.

You configure the route-based VPN parameters described in Table 20 on page 241.

Table 20: 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

Table 20: User Logical System Route-Based VPN Configuration *(Continued)*

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

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set interfaces 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

IN THIS SECTION

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 12.1.1.0/24 subnet in the ls-product-design user logical system to the host 192.168.168.10.

Verifying the IKE Phase 1 Status

Purpose

Verify the IKE Phase 1 status.

Action

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

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

Verifying the IPsec Phase 2 Status

Purpose

Verify the IPsec Phase 2 status.

Action

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

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

SEE ALSO

- Example: Configuring a Route-Based VPN
- Understanding Route-Based VPN Tunnels in Logical Systems | 229
- User Logical Systems Configuration Overview | 48

RELATED DOCUMENTATION

- IPv6 Addresses in Logical Systems Overview | 356

Content Security for Logical Systems

IN THIS SECTION

Content Security provides multiple security features and services for SRX Series Firewalls on the network, protecting users from security threats in a simplified way. Content Security secures the logical systems from viruses, malware, or malicious attachments by scanning the incoming data using Deep Packet Inspection and prevents access to unwanted websites by installing Enhanced Web Filtering (EWF).

Understanding Content Security Features in Logical Systems

Content Security in logical systems provides several security features such as antispam, antivirus, content filtering, and Web filtering to secure users from multiple Internet-borne threats. The advantage of Content Security is streamlined installation and management of these multiple security capabilities. In logical systems the primary administrator configures the Content Security features for the primary logical system. Configuring Content Security features for logical systems is similar to configuring Content Security features on a device that is not configured for logical systems.

The security features provided as part of the Content Security solution are:

- *Antispam Filtering*—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. The default antispam feature is configured at the primary logical system and it is applicable for all the user logical systems.
- *Content Filtering*—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. The default content filtering feature is configured at the primary logical system and it is applicable for all the user logical systems.
- *Web Filtering*—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. The default Web filtering feature is configured at the primary logical system, and the user logical systems inherit these default Web filtering configuration.
- *Sophos Antivirus*—Sophos Antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. Sophos Antivirus is as an in-the-cloud antivirus solution. The default antivirus feature is configured at the primary logical system, and the user logical systems inherit these default antivirus configuration.

You must configure the custom objects for the Web filtering, anti-spam, and content filtering features before configuring the Content Security features. You can configure custom objects for each user logical system.

The predefined Content Security default policy parameters for Web filtering, content filtering, antivirus, and antispam profiles are configured at the primary logical system. The user logical systems inherit the same antivirus and Web filtering features configured for the primary logical system. The options such as `mime-whitelist` and `url-whitelist` in antivirus profile, and `address-blacklist` and `address-whitelist` in antispam profile can be configured at the following hierarchy levels, respectively:

- `[edit security utm feature-profile anti-virus sophos-engine profile]`
- `[edit security utm feature-profile anti-spam sbl profile]`

The options `url-whitelist` and `url-blacklist` are not supported in the Web fiterling profile, you can use the custom category option to achieve the function.

Example: Configuring Content Security for the Primary Logical System

IN THIS SECTION

This example shows how to configure the Content Security features antivirus, antispam, content filtering, and Web filtering in the primary logical system. The primary administrator is responsible for assigning the Content Security features to the user logical systems.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall configured with the logical systems.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand how to log in to the primary logical system as the primary administrator. See "Primary Logical Systems Overview" on page 20.
- Configure the interfaces, routing instances, and static routes for the primary logical system. See "Example: Configuring Interfaces, Routing Instances, and Static Routes for the Primary and Interconnect Logical Systems and Logical Tunnel Interfaces for the User Logical Systems (Primary Administrators Only)" on page 111.

Overview

By default, all system resources are assigned to the primary logical system, and the primary administrator allocates them to the user logical systems. The primary administrator manages the device and the logical systems.

This example shows how to configure the Content Security features described in Table 21 on page 249 for the primary logical system.

Table 21: Content Security Configuration Type, Steps, and Parameters

Configuration Type	Configuration Description	Configuration Parameter
Custom objects	Configure the MIME (Multipurpose Internet Mail Extension) types (`my_blockmime01`) to decide which traffic is allowed to bypass various types of scanning	*[multipart/ application/]*
	Define a set of file extensions (`my_fileextlist01`) that are used in file extension scan mode (scan-by-extension)	*[txt pl com zip]*
	Configure a URL pattern list (`black_list`) of URLs or addresses that you want to block.	*www.example.com*
	Configure a custom URL category (`cust_black`) of URLs or addresses that you want to block.	*black_list*
Antispam	Configure the antispam type server-based spam block list (SBL).	*sbl*
Antivirus	Configure the antivirus type Sophos Antivirus (`sophos-engine`) profile (`mysav`) scan option to scan specific types of traffic.	*uri-check*
Web filtering	Specify an action for Enhanced Web Filtering (EWF) (`juniper-enhanced`) profile (`myewf`), for requests that experience internal errors in the Web filtering module.	*log-and-permit*

In this procedure, you define custom objects, configure feature profiles for Content Security features (antispam, antivirus, content filtering, and Web filtering), configure a Content Security policy and attach feature profiles, and apply the Content Security policy to the security policy as an application service. For more information, see the Unified Threat Management User Guide.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set security utm custom-objects mime-pattern my_blockmime01 value [ multipart/ application/ ]
set security utm custom-objects filename-extension my_fileextlist01 value [ txt pl com zip ]
set security utm custom-objects url-pattern black_list value www.example.com
set security utm custom-objects custom-url-category cust_black value black_list
set security utm default-configuration anti-virus type sophos-engine
set security utm default-configuration web-filtering type juniper-enhanced
set security utm default-configuration web-filtering juniper-enhanced cache timeout 1800
set security utm default-configuration web-filtering juniper-enhanced cache size 0
set security utm default-configuration anti-spam type sbl
set security utm feature-profile anti-virus sophos-engine profile mysav scan-options uri-check
set security utm feature-profile web-filtering juniper-enhanced profile myewf default log-and-
permit
set security utm utm-policy utm-p1 anti-virus http-profile mysav
set security utm utm-policy utm-p1 content-filtering http-profile junos-cf-defaults
set security utm utm-policy utm-p1 web-filtering http-profile myewf
set security utm utm-policy utm-p1 anti-spam smtp-profile junos-as-defaults
set security policies from-zone trust to-zone untrust policy p1 match source-address any
set security policies from-zone trust to-zone untrust policy p1 match destination-address any
set security policies from-zone trust to-zone untrust policy p1 match application junos-http
set security policies from-zone trust to-zone untrust policy p1 then permit application-services
utm-policy utm-p1
```

Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the Junos OS CLI User Guide.

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

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

2. Configure the custom objects for the primary logical system.

```
[edit security utm custom-objects]
admin@host# set mime-pattern my_blockmime01 value [ multipart/ application/ ]
admin@host# set filename-extension my_fileextlist01 value [ txt pl com zip ]
admin@host# set url-pattern black_list value www.example.com
admin@host# set custom-url-category cust_black value black_list
```

3. Define the Content Security default configuration for the primary logical system.

```
[edit security utm default-configuration]
admin@host# set anti-virus type sophos-engine
admin@host# set web-filtering type juniper-enhanced
admin@host# set web-filtering juniper-enhanced cache timeout 1800
admin@host# set web-filtering juniper-enhanced cache size 0
admin@host# set anti-spam type sbl
```

4. Configure the feature profile for the primary logical system.

```
[edit security utm feature-profile]
admin@host# set anti-virus sophos-engine profile mysav scan-options uri-check
admin@host# set web-filtering juniper-enhanced profile myewf default log-and-permit
```

5. Configure the Content Security policy for the primary logical system.

```
[edit security utm utm-policy]
admin@host# set utm-p1 anti-virus http-profile mysav
admin@host# set utm-p1 content-filtering http-profile junos-cf-defaults
admin@host# set utm-p1 web-filtering http-profile myewf
admin@host# set utm-p1 anti-spam smtp-profile junos-as-defaults
```

6. Configure the security policies for the primary logical system.

```
[edit security policies]
admin@host# set from-zone trust to-zone untrust policy p1 match source-address any
admin@host# set from-zone trust to-zone untrust policy p1 match destination-address any
admin@host# set from-zone trust to-zone untrust policy p1 match application junos-http
admin@host# set from-zone trust to-zone untrust policy p1 permit application-services utm-
policy utm-p1
```

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.

```
admin@host# show security
utm {
    custom-objects {
        mime-pattern {
            my_blockmime01 {
                value [ multipart/ application/ ];
            }
        }
        filename-extension {
            my_fileextlist01 {
                value [ txt pl com zip ];
            }
        }
        url-pattern {
            black_list {
                value www.example.com;
            }
```

```
        }
        custom-url-category {
            cust_black {
                value black_list;
            }
        }
    }
    default-configuration {
        anti-virus {
            type sophos-engine;
        }
        web-filtering {
            type juniper-enhanced;
            juniper-enhanced {
                cache {
                    timeout 1800;
                    size 0;
                }
            }
        }
        anti-spam {
            type sbl;
        }
    }
    feature-profile {
        anti-virus {
            sophos-engine {
                profile mysav {
                    scan-options {
                        uri-check;
                    }
                }
            }
        }
        web-filtering {
            juniper-enhanced {
                profile myewf {
                    default log-and-permit;
                }
            }
        }
    }
    utm-policy utm-p1 {
```

```
        anti-virus {
            http-profile mysav;
        }
        content-filtering {
            http-profile junos-cf-defaults;
        }
        web-filtering {
            http-profile myewf;
        }
        anti-spam {
            smtp-profile junos-as-defaults;
        }
    }
}
policies {
    from-zone trust to-zone untrust {
        policy p1 {
            match {
                source-address any;
                destination-address any;
                application junos-http;
            }
            then {
                permit {
                    application-services {
                        utm-policy utm-p1;
                    }
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying Antivirus Configuration

Purpose

Verify that the antivirus feature is configured for the primary logical system.

Action

From operational mode, enter the `show security utm anti-virus statistics` command to view the details of the antivirus feature configured for the primary logical system.

```
admin@host> show security utm anti-virus statistics
 UTM Anti Virus statistics:
 MIME-whitelist passed:                0
URL-whitelist passed:                 0
Session abort:                        0
Scan Request:

  Total           Clean         Threat-found    Fallback
      9               7              1               1

Fallback:
                       Log-and-Permit    Block       Permit
Engine not ready:          0                0           0
 Out of resources:         0                0           0
Timeout:                   0                0           0
Maximum content size:      1                0           0
Too many requests:         0                0           0
Others:                    0                0           0
```

Meaning

The output displays the antisvirus statistics for the primary logical system.

Verifying Antispam Configuration

Purpose

Verify that the antispam feature is configured for the primary logical system.

Action

From operational mode, enter the `show security utm anti-spam statistics` command to view the details of the antispam feature configured for the primary logical system.

```
admin@host> show security utm anti-spam statistics
 UTM Anti Spam statistics:

Total connections:     1
Denied connections:    1
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

Meaning

The output displays the antispam statistics for the primary logical system.

Verifying Content Filtering Configuration

Purpose

Verify that the content filtering feature is configured for the primary logical system.

Action

From operational mode, enter the `show security utm content-filtering statistics` command to view the details of the content filtering feature configured for the primary logical system.

```
admin@host> show security content-filtering statistics
 Content-filtering-statistic:         Blocked
     Base on command list:                    0
     Base on mime list:                       1
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
     EXE files:                               0
     ZIP files:                               0
     HTTP cookie:                             0
```

Meaning

The output displays the content filtering statistics for the primary logical system.

Verifying Web Filtering Configuration

Purpose

Verify that the Web filtering feature is configured for the primary logical system.

Action

From operational mode, enter the `show security utm web-filtering statistics` command to view the details of the Web filtering feature configured for the primary logical system.

```
admin@host> show security web-filtering statistics
 UTM web-filtering statistics:
    Total requests:                    4
```

```
    white list hit:                    1
    Black list hit:                    1
    Custom category permit:            1
    Custom category block:             1
    Custom category quarantine:        0
    Custom category qurantine block:   0
    Custom category quarantine permit: 0
    Web-filtering sessions in total:   64000
    Web-filtering sessions in use:     0
    Fallback:                  log-and-permit     block
          Default                           0         0
          Timeout                           0         0
     Connectivity                           0         0
Too-many-requests                           0         0
```

Meaning

The output displays the Web filtering statistics for the primary logical system.

Example: Configuring Content Security for a User Logical System

IN THIS SECTION

This example shows how to configure the Content Security features antivirus, antispam, content filtering, and Web filtering for a user logical system. The primary administrator creates a user logical system and assigns an administrator for managing the user logical system. A user logical system can have multiple user logical system administrators.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall configured with the logical systems.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand the user logical system administrator role and functions. See "Understanding User Logical Systems and the User Logical System Administrator Role" on page 50.
- Understand how to log in to the user logical system as an administrator. See "User Logical Systems Configuration Overview" on page 48.
- This example shows how to configure the Content Security features for the ls-product-design user logical system. To understand how to create the ls-product-design user logical system, see "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54.

Overview

The primary administrator assigns the Content Security features antivirus, antispam, content filtering, and Web filtering to the user logical system. The user logical system administrator can configure and manage the Content Security features for the user logical systems. The antispam, antivirus and Web filtering features are configured in the primary logical system are described in Table 22 on page 259. All the user logical systems can use the same antispam, antivirus and Web filtering features with the same profile.

Table 22: Content Security Configuration Type, Steps, and Parameters

Configuration Type	Configuration Description	Configuration Parameter
Custom objects	Configure a URL pattern (`url1`) of URL patterns that bypass scanning.	*www.abc.com*
	Configure a custom URL category (`cust1`) of URLs or addresses list that bypass scanning.	*url1*
	Configure a custom message type (`redirect-url`) to redirect traffic destined for protected sources.	*http://www.example1.com.cn*

Table 22: Content Security Configuration Type, Steps, and Parameters *(Continued)*

Configuration Type	Configuration Description	Configuration Parameter
Antispam	Configure antispam profile (as1) spam action.	*block*
Antivirus	Configure antivirus profile (sav1) fallback option.	*log-and-permit*
	Configure antivirus profile (sav1) scan option.	*uri-check*
Web filtering	Configure Web filtering profile (ewf1) category (cust1) action.	*block*
	Configure Web filtering profile (ewf1) category (cust1) custom message.	*custmsg1*
	Configure Web filtering profile (ewf1) category (Enhanced_Search_Engines_and_Portals) action.	*block*
	Specify an action for Enhanced Web Filtering (EWF) (juniper-enhanced) profile (ewf1), for requests that experience internal errors in the Web filtering module.	*log-and-permit*

Configuration

IN THIS SECTION

CLI Quick Configuration

To quickly configure this example, log in to the ls-product-design user logical system as the administrator, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set security utm custom-objects url-pattern url1 value www.abc.com
set security utm custom-objects custom-url-category cust1 value url1
set security utm custom-objects custom-message cust-msg1 type redirect-url content http://
www.example1.com.cn
set security utm feature-profile anti-virus sophos-engine profile sav1 fallback-options default
log-and-permit
set security utm feature-profile anti-virus sophos-engine profile sav1 scan-options uri-check
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category cust1
action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category cust1
custom-message custmsg1
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 category
Enhanced_Search_Engines_and_Portals action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf1 default log-and-
permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf2 default log-and-
permit
set security utm feature-profile anti-spam sbl profile as1 spam-action block
set security utm utm-policy utm-p1 anti-virus http-profile sav1
set security utm utm-policy utm-p1 web-filtering http-profile juniper-enhanced
set security utm utm-policy utm-p1 anti-spam smtp-profile as1
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust policy
sec_policy match source-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust policy
sec_policy match destination-address any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust policy
sec_policy match application any
set security policies from-zone ls-product-design-trust to-zone ls-product-design-untrust policy
sec_policy then permit application-services utm-policy utm-p1
```

Procedure

Step-by-Step Procedure

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

1. Log in to the ls-product-design user logical system as the administrator and enter configuration mode.

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

2. Configure the custom objects for the ls-product-design user logical system.

```
[edit security utm custom-objects]
lsdesignadmin1@host:ls-product-design# set url-pattern url1 value www.abc.com
lsdesignadmin1@host:ls-product-design# set custom-url-category cust1 value url1
lsdesignadmin1@host:ls-product-design# set custom-message cust-msg1 type redirect-url content
http://www.example1.com.cn
```

3. Configure the feature profiles for the ls-product-design user logical system.

```
[edit security utm feature-profile]
lsdesignadmin1@host:ls-product-design# set anti-virus sophos-engine profile sav1 fallback-
options default log-and-permit
lsdesignadmin1@host:ls-product-design# set anti-virus sophos-engine profile sav1 scan-options
uri-check
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile ewf1
category cust1 action block
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile ewf1
category cust1 custom-message custmsg1
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile ewf1
category Enhanced_Search_Engines_and_Portals action block
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile ewf1
default log-and-permit
lsdesignadmin1@host:ls-product-design# set web-filtering juniper-enhanced profile ewf2
default log-and-permit
lsdesignadmin1@host:ls-product-design# set anti-spam sbl profile as1 spam-action block
```

4. Configure the Content Security policy for the ls-product-design user logical system.

```
[edit security utm utm-policy]
lsdesignadmin1@host:ls-product-design# set utm-p1 anti-virus http-profile sav1
lsdesignadmin1@host:ls-product-design# set utm-p1 web-filtering http-profile juniper-enhanced
lsdesignadmin1@host:ls-product-design# set utm-p1 anti-spam smtp-profile as1
```

5. Configure the security policies for the ls-product-design user logical system.

```
[edit security policies]
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone lsys1-untrust policy
sec_policy match source-address any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone lsys1-untrust policy
sec_policy match destination-address any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone lsys1-untrust policy
sec_policy match application any
lsdesignadmin1@host:ls-product-design# set from-zone lsys1-trust to-zone lsys1-untrust policy
sec_policy then permit application-services utm-policy utm-p1
```

Results

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

```
lsdesignadmin1@host:ls-product-design# show security
utm {
    custom-objects {
        url-pattern {
            url1 {
                value www.abc.com;
            }
        }
        custom-url-category {
            cust1 {
                value url1;
            }
        }
        custom-message {
            cust-msg1 {
```

```
                type redirect-url;
                content http://www.example1.com.cn;
            }
        }
    }
    feature-profile {
        anti-virus {
            sophos-engine {
                profile sav1 {
                    fallback-options {
                        default log-and-permit;
                    }
                    scan-options {
                        uri-check;
                    }
                }
            }
        }
        web-filtering {
            juniper-enhanced {
                profile ewf1 {
                    category {
                        cust1 {
                            action block;
                            custom-message custmsg1;
                        }
                        Enhanced_Search_Engines_and_Portals {
                            action block;
                        }
                    }
                    default log-and-permit;
                }
                profile ewf2 {
                    default log-and-permit;
                }
            }
        }
        anti-spam {
            sbl {
                profile as1 {
                    spam-action block;
                }
            }
```

```
        }
    }
    utm-policy utm-p1 {
        anti-virus {
            http-profile sav1;
        }
        web-filtering {
            http-profile juniper-enhanced;
        }
        anti-spam {
            smtp-profile as1;
        }
    }
}
policies {
    from-zone ls-product-design-trust to-zone ls-product-design-untrust {
        policy sec_policy {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        utm-policy utm-p1;
                    }
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying Antivirus Configuration

Purpose

Verify that the antivirus feature is configured for the ls-product-design user logical system.

Action

From operational mode, enter the `show security utm anti-virus statistics` command to view the antivirus statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security utm anti-virus statistics
 UTM Anti Virus statistics:
 MIME-whitelist passed:                0
URL-whitelist passed:                 0
Session abort:                        0
Scan Request:

  Total           Clean         Threat-found    Fallback
    9               7             1               1

Fallback:
                       Log-and-Permit    Block       Permit
Engine not ready:          0                 0           0
 Out of resources:         0                 0           0
Timeout:                   0                 0           0
Maximum content size:      1                 0           0
Too many requests:         0                 0           0
Others:
```

Meaning

The output displays the antisvirus statistics information for the ls-product-design user logical system.

Verifying Antispam Configuration

Purpose

Verify that the antispam feature is configured for the ls-product-design user logical system.

Action

From operational mode, enter the `show security utm anti-spam statistics` command to view the antispam statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security utmnti-spam statistics
 UTM Anti Spam statistics:

Total connections:     1
Denied connections:    1
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

Meaning

The output displays the antispam statistics information for the ls-product-design user logical system.

Verifying Content Filtering Configuration

Purpose

Verify that the content filtering feature is configured for the ls-product-design user logical system.

Action

From operational mode, enter the `show security utm content-filtering statistics` command to view the content filtering statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security content-filteringtatistics
 Content-filtering-statistic:         Blocked
     Base on command list:                    0
     Base on mime list:                       1
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
     EXE files:                               0
     ZIP files:                               0
     HTTP cookie:                             0
```

Meaning

The output displays the content filtering statistics information for the ls-product-design user logical system.

Verifying Web Filtering Configuration

Purpose

Verify that the Web filtering feature is configured for the ls-product-design user logical system.

Action

From operational mode, enter the `show security utm web-filtering statistics` command to view the Web filtering statistics information for the ls-product-design user logical system.

```
lsdesignadmin1@host:ls-product-design> show security web-filteringstatistics
 UTM web-filtering statistics:
```

```
    Total requests:                    4
    white list hit:                    1
    Black list hit:                    1
    Custom category permit:            1
    Custom category block:             1
    Custom category quarantine:        0
    Custom category qurantine block:   0
    Custom category quarantine permit: 0
    Web-filtering sessions in total:   64000
    Web-filtering sessions in use:     0
    Fallback:         log-and-permit          block
          Default                  0              0
          Timeout                  0              0
     Connectivity                  0              0
Too-many-requests                  0              0
```

Meaning

The output displays the Web filtering statistics information for the ls-product-design user logical system.

IDP for Logical Systems

IN THIS SECTION

An Intrusion Detection and Prevention (IDP) policy in logical systems enables you to selectively enforce various attack detection and prevention techniques on the network traffic passing through your SRX Series. The SRX Series offer the same set of IDP signatures that are available on Juniper Networks IDP

Series Intrusion Detection and Prevention Appliances to secure networks against attacks. For more information, see the following topics:

IDP in Logical Systems Overview

IN THIS SECTION

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

This topic includes the following sections:

IDP Policies

The primary 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.

IDP policy templates installed in root logical system are visible and used by all logical systems.

The primary 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 primary 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 primary administrator can configure multiple IDP policies, a logical system can have only one active IDP policy at a time. For user logical systems, the primary 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 primary logical system, the primary administrator can *either* reference the IDP policy in the security profile that is bound to the primary logical system or use the `active-policy` *configuration statement* at the [`edit security idp`] hierarchy level.

The root administrator configures the number of maximum IDP sessions reservation for a root and user logical system. The number of IDP sessions that are allowed for a root logical system are defined using

the command `set security idp max-sessions` *`max-sessions`* and the number of IDP sessions that are allowed for a user logical system are defined using the command `set security idp logical-system` *`logical-system`* `max-sessions` *`max-sessions`*.

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

NOTE: If you have configured more than one IDP policy in a security policy, then configuring default IDP policy configuration is mandatory.

A default IDP policy configuration is supported when multiple IDP policies are available. The default IDP policy is one of the multiple IDP policies. For more information about configuring multiple IDP policies and default IDP policy, see the *IDP Policy Selection for Unified Policies*.

The logical system administrator performs the following actions:

- Configure multiple IDP policies and attach to the firewall policies to be used by the user logical systems. If the IDP policy is not configured for a user logical system, the default IDP policy configured by the primary administrator is used. The IDP policy is bound to the user logical systems through a logical systems security policy.
- Create or modify IDP policies for their user logical systems. The IDP policies are bound to user logical systems. When an IDP policy is changed, and commit succeeds, the existing sessions mapped to current active policy continue to use the old IDP combined policy. When an IDP policy is changed, and commit fails, only the logical system user that has initiated the commit change is notified about the commit failure.
- The logical system 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 primary administrator. The primary administrator can reference zones in the primary logical system in an IDP policy configured for the primary logical system.
- View the attack statistics detected and IDP counters, attack table, and policy commit status by the individual logical system using the commands `show security idp counters`, `show security idp attack table`, `show security idp policies`, `show security idp policy-commit-status`, and `show security idp security-package-version`.

Limitation

- When a IDP policy is changed and compiled in a specific user logical system, this change is considered as a single global policy change and compiled for all policies of all the logical systems.

IDP Installation and Licensing for 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.

A single IDP security package is installed for all logical systems on the device at the root level. 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.

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68

IDP Policies Overview

Understanding IDP Features in Logical Systems

IN THIS SECTION

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 primary 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 primary 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 primary 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 primary 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:

```
Feb 22 14:06:00 aqgpo1ifw01 RT_IDP: %-IDP_ATTACK_LOG_EVENT_LS: Lsys A01: IDP: At 1329883555,
ANOMALY Attack log <10.1.128.200/33699->192.168.22.84/80> for TCP protocol and service HTTP
application NONE by rule 4 of rulebase IPS in policy Policy1. attack: repeat=3, action=NONE,
threat-severity=INFO, name=HTTP:AUDIT:URL, NAT <0.0.0.0:0->0.0.0.0:0>, time-elapsed=0,
inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:NSS-Mgmt:reth0.55->SIEM-MGMT:reth0.60,
packet-log-id: 0 and misc-message
```

NOTE: In the IDP attack detection event log message (IDP_ATTACK_LOG_EVENT_LS), the time-elapsed, inbytes, outbytes, inpackets, and outpackets fields are not populated.

- 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
```

SEE ALSO

Understanding IDP Policy Rule Bases

Understanding IDP Protocol Decoders

IDP SSL Overview

Understanding IDP Inline Tap Mode

Understanding Multiple IDP Detector Support

Understanding IDP Logging

Example: Configuring an IDP Policy for the Primary Logical Systems

IN THIS SECTION

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

Requirements

Before you begin:

- Log in to the primary logical system as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.
- Read "IDP in Logical Systems Overview" on page 270.
- Use the `show system security-profile` command to see the resources allocated to the primary logical system.

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 primary logical system. IDP is then enabled in a security policy configured in the primary logical system.

You configure the features described in Table 23 on page 277.

Table 23: IDP Configuration for the Primary 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	primary-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 primary logical system, the primary administrator can reference the IDP policy in the security profile that is bound to the primary logical system as

shown in this example. Alternatively, the primary 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 primary logical system and specified with the `active-policy` configuration statement. Use only one method to specify the active IDP policy for the primary logical system.

Configuration

IN THIS SECTION

Configuring a Custom Attack

CLI Quick Configuration

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

```
set security 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 primary logical system as the primary 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 Primary Logical System

CLI Quick Configuration

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

```
set security 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 root-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*.

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

```
set security policies 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

IN THIS SECTION

- Verifying Attack Matches | 284

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
```

SEE ALSO

IDP in Logical Systems Overview | 270

SRX Series Logical Systems Primary Administrator Configuration Tasks Overview | 22

Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System

IN THIS SECTION

The primary 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 primary

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 primary logical system as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.
- Read *IDP Policies Overview*.
- Assign the ls-design-profile security policy to the ls-product-design user logical system. See "Example: Configuring Logical Systems Security Profiles (Primary Administrators Only)" on page 74.
- Download predefined IDP policy templates to the device. See *Downloading and Using Predefined IDP Policy Templates (CLI Procedure)*.

> **NOTE**: Activating a predefined IDP policy with the `active-policy` configuration statement at the [`edit security idp`] hierarchy level only applies to the primary logical system. For a user logical system, the primary 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 54.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set 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 primary logical system as the primary 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

IN THIS SECTION

- Verifying the Configuration | 287

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
```

SEE ALSO

Example: Enabling IDP in a User Logical System Security Policy | 288

IDP in Logical Systems Overview | 270

Example: Enabling IDP in a User Logical System Security Policy

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- From configuration mode, use the `show system security-profile <profile-name> idp-policy` command to see the security policy resources allocated to the logical system.
- Configure an IDP security policy for the user logical system as the primary administrator. See "Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System" on page 284.

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 54.

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 primary administrator in "Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System" on page 284.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security policies 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

IN THIS SECTION

- Verifying Attack Matches | **291**

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
```

SEE ALSO

Example: Configuring and Assigning a Predefined IDP Policy for a User Logical System | **284**

IDP in Logical Systems Overview | **270**

Example: Configuring an IDP Policy for a User Logical System

IN THIS SECTION

This example shows how to configure and assign an IDP policy to a user logical system. After assigning the IDP policy, the traffic is sent from client to check for the attack detection on the configured custom attack.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 18.3R1 and later
- an SRX4200 device

Before you configure IDP policy on user logical system:

- Configure security zones. See "Example: Configuring Security Zones for a User Logical Systems" on page 163.

Overview

In this example, you configure a custom attack that is used in an IDP policy. The IDP policy is specified and enabled using a security policy configured in the user logical system.

Configuration

IN THIS SECTION

To configure IDP in a user logical system:

Configuring a user logical system

CLI Quick Configuration

Step-by-Step Procedure

To configure a user logical system:

1. Configure a user logical system.

```
[edit]
user@host# set logical-system LSYS1
```

2. Exit from the configuration mode and enter to the operational mode.

```
user@host# exit
```

3. Login as LSYS1 user to the user logical sytem and enter to configuration mode.

```
user@host> set cli logical-system LSYS1
user@host:LSYS1> edit
user@host:LSYS1#
```

Results

From configuration mode, confirm your configuration by entering the `show logical-systems` 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
    LSYS1 {
    }
```

Configuring a Custom Attack

CLI Quick Configuration

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

```
set security idp custom-attack my-http severity info
set security idp custom-attack my-http attack-type signature protocol-binding application HTTP
set security idp custom-attack my-http attack-type signature context http-get-url
set security idp custom-attack my-http attack-type signature pattern .*test.*
set security idp custom-attack my-http attack-type signature direction any
```

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 user logical system as LSYS1 and enter configuration mode.

```
[edit]
user@host:LSYS1#
```

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

```
[edit security idp]
user@host:LSYS1# set custom-attack my-http severity info
```

3. Configure stateful signature parameters.

```
[edit security idp]
user@host:LSYS1# set custom-attack my-http attack-type signature protocol-binding application
HTTP
user@host:LSYS1# set custom-attack my-http attack-type signature context http-get-url
user@host:LSYS1# set custom-attack my-http attack-type signature pattern .*test.*
user@host:LSYS1# set custom-attack my-http attack-type signature direction any
```

Results

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

```
[edit]
user@host:LSYS1# show security idp custom-attack my-http
severity info;
    attack-type {
    signature {
        protocol-binding {
            application HTTP;
        }
        context http-get-url;
        pattern .*test.*;
        direction any;
    }
}
```

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

Configuring an IDP Policy for the User Logical System

CLI Quick Configuration

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

```
set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match application default
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-attacks my-http
set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
```

Step-by-Step Procedure

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

To configure an IDP policy:

1. Create the IDP policy and configure match conditions.

```
[edit security idp]
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match from-zone any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match source-address any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match destination-address any
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match application default
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks custom-attacks my-
http
```

2. Configure actions for the IDP policy.

```
[edit security idp]
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host:LSYS1# set idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
```

Results

From configuration mode, confirm your configuration by entering the `show security idp idp-policy idpengine` 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]
user@host:LSYS1# show security idp idp-policy idpengine
rulebase-ips {
    rule 1 {
        match {
            from-zone any;
            source-address any;
            to-zone any;
            destination-address any;
            application default;
            attacks {
                custom-attacks my-http;
            }
        }
        then {
            action {
                no-action;
            }
            notification {
                log-attacks;
            }
        }
    }
}
```

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

```
set security policies from-zone z1 to-zone z2 policy p1 match source-address any
set security policies from-zone z1 to-zone z2 policy p1 match destination-address any
set security policies from-zone z1 to-zone z2 policy p1 match application any
set security policies from-zone z1 to-zone z2 policy p1 then permit application-services idp-
policy idpengine
```

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 z1 to-zone z2]
user@host:LSYS1# set policy p1 match source-address any
user@host:LSYS1# set policy p1 match destination-address any
user@host:LSYS1# set policy p1 match application any
```

2. Enable IDP.

```
[edit security policies from-zone z1 to-zone z2]
user@host:LSYS1# set policy p1 then permit application-services idp-policy idpengine
```

Results

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

```
[edit]
user@host:LSYS1# show security policies
```

```
from-zone z1 to-zone z2 {
    policy p1{
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    idp-policy idpengine;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

- Verifying Attack Detection | 299

To send traffic and check for attack detection from user logical system:

Verifying Attack Detection

Purpose

Verify that attack detection is happening for the custom attack.

Action

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

```
user@host:LSYS1> show security idp policies
 PIC : FPC 0 PIC 0:
```

```
ID    Name                  Sessions    Memory      Detector
 1     idpengine             0           188584      12.6.130180509
```

```
user@host:LSYS1> show security idp attack table
IDP attack statistics:

  Attack name                                  #Hits
  my-http                                          1
```

Meaning

The output displays the attacks detected for the custom attack that is configured in the IDP policy in the user logical system LSYS1.

SEE ALSO

idp

ALG for Logical Systems

IN THIS SECTION

An Application Layer Gateway (ALG) in logical systems enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server. ALGs supports the applications such as Transfer Protocol (FTP) and various IP protocols that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. For more information, see the following topics:

Understanding Application Layer Gateway (ALG) in Logical Systems

The primary administrator can configure ALGs at the root level. The configuration is inherited by all user logical systems. ALGs can also be configured discretely for user logical systems. The ALG status is not inherited by all user logical systems. For a newly created logical system, the ALG consists of a default status. The FTP protocol ALG can be enabled or disabled for a specific logical system. The ICMP ALG protocol is enabled by default and is not provisioned to disable.

NOTE: When an SRX Series Firewall is upgraded to 18.2 release, the ALG status in a logical system is changed when compared with previous status. This change affects the ALG traffic in the logical system. For example, before upgrade, H.323 ALG is configured to enable by root. So H.323 ALG is also enabled in lsys1. After upgrade to 18.2, H.323 ALG status in lsys1 is disabled because the default status for H.323 is disabled for a new logical system.

NOTE: You can enable a particular ALG for only one specific logical system.

By default, the following ALGs are enabled on a root logical system:

- DNS
- FTP
- MSRPC
- PPTP
- SUNRPC
- TALK
- TFTP

Starting in Junos OS Release 18.2R1, you can either enable or disable the ALGs configuration for each logical system individually, and view the status of the ALGs for all logical systems or specific logical system. All 12 data ALGs (DNS, FTP, TFTP, MSRPC, SUNRPC, PPTP, RSH, RTSP, TALK, SQL, IKE, and TWAMP) and four VOIP ALGs (SIP, H.323, MGCP, and SCCP) are supported on the logical systems.

SEE ALSO

show security alg status logical-system

Example: Enabling FTP ALG in a Logical System | 307

alg

Enabling and Disabling ALG for Logical System

This topic shows how to enable or disable the ALG status for each logical system.

1. By Default IKE ALG is disabled on the logical system. To enable this ALG, use the following command.
   - Enable IKE and ESP ALG with NAT.

```
[edit]
user@host# set logical-systems LSYS1 security alg ike-esp-nat enable
```

2. By default, the DNS, FTP, PPTP, SIP, SUNRPC and TWAMP ALGs are enabled on the logical system. To disable these ALGs, use the following commands.
   - Disable DNS ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg dns disable
```

   - Disable FTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg ftp disable
```

   - Disable H323 ALG.

```
[edit]
user@host# logical-systems LSYS1 security alg h323 disable
```

   - Disable MGCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg mgcp disable
```

- Disable MSRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg msrpc disable
```

- Disable PPTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg pptp disable
```

- Disable RSH ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rsh disable
```

- Disable RTSP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rtsp disable
```

- Disable SCCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sccp disable
```

- Disable SIP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sip disable
```

- Disable SQL ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sql disable
```

- Disable SUNRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sunrpc disable
```

- Disable TALK ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg talk disable
```

- Disable TFTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg tftp disable
```

3. Configuring ALG functions in logical systems.

- Configure DNS ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg dns
```

- Configure FTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg ftp
```

- Configure H323 ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg h323
```

- Configure IKE and ESP ALG with NAT.

```
[edit]
user@host# set logical-systems LSYS1 security alg ike-esp-nat
```

- Configure MGCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg mgcp
```

- Configure MSRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg msrpc
```

- Configure PPTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg pptp
```

- Configure RSH ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rsh
```

- Configure RTSP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg rtsp
```

- Configure SCCP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sccp
```

- Configure SIP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sip
```

- Configure SQL ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sql
```

- Configure SUNRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sunrpc
```

- Configure TALK ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg talk
```

- Configure TFTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg tftp
```

- Configure TWAMP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg twamp
```

- Configure extended function for FTP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg ftp allow-mismatch-ip-address
```

- Configure extended function for MSRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg msrpc map-entry-timeout 10
```

- Configure extended function for SUNRPC ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sunrpc map-entry-timeout 10
```

- Configure extended function for SIP ALG.

```
[edit]
user@host# set logical-systems LSYS1 security alg sip retain-hold-resource
```

Example: Enabling FTP ALG in a Logical System

IN THIS SECTION

This example shows how to enable or disable an FTP ALG configuration in a logical system and send traffic based on FTP ALG configuration of the logical system individually.

Requirements

Before you begin:

- Log in to the user logical system as the logical system administrator. See "User Logical Systems Configuration Overview" on page 48.

Overview

In this example, the ALG for FTP is configured to monitor and allow FTP traffic to be exchanged between the clients and the server on a logical system.

By default, the FTP ALG is enabled on the logical system.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50
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 routing-instances vr0 instance-type vpls
set logical-systems LSYS0 routing-instances vr0 interface lt-0/0/0.0
set system security-profile p1 logical-system LSYS0
set system security-profile p1 logical-system LSYS1
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 0
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 10.0.0.0/8
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet address 198.51.100.0/24
set logical-systems LSYS1 interfaces ge-0/0/1 unit 0 family inet address 203.0.113.0/24
set logical-systems LSYS1 security zones security-zone LSYS1_tzone host-inbound-traffic system-
services all
set logical-systems LSYS1 security zones security-zone LSYS1_tzone host-inbound-traffic protocol
all
set logical-systems LSYS1 security zones security-zone LSYS1_tzone interfaces ge-0/0/0
```

```
set logical-systems LSYS1 security zones security-zone LSYS1_utzone host-inbound-traffic system-
services all
set logical-systems LSYS1 security zones security-zone LSYS1_utzone host-inbound-traffic
protocol all
set logical-systems LSYS1 security zones security-zone LSYS1_utzone interfaces ge-0/0/1
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone policy
p11 match source-address any
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone policy
p11 match destination-address any
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone policy
p11 match application junos-ftp
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone policy
p11 match application junos-ping
set logical-systems LSYS1 security policies from-zone LSYS1_tzone to-zone LSYS1_utzone policy
p11 then permit
set logical-systems LSYS1 security policies default-policy deny-all
```

Configuring FTP ALG in a 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.

To configure an ALG in a user logical system:

1. Configure a security profile.

```
[edit system security-profile]
user@host#set p1 policy maximum 100
user@host#set p1 policy reserved 50
user@host#set p1 zone maximum 100
user@host#set p1 zone reserved 50
user@host#set p1 flow-session maximum 6291456
user@host#set p1 flow-session reserved 50
user@host#set p1 flow-gate maximum 524288
user@host#set p1 flow-gate reserved 50
```

2. Configure the primary logical system.

Step-by-Step Procedure

a. Create the primary logical system

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

b. Configure interfaces for a primary logical system and configure logical tunnel interfaces and routing instances to the LSYS0.

```
[edit 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 routing-instances vr0 instance-type vpls
user@host#set routing-instances vr0 interface lt-0/0/0.0
```

c. Configure a security profile p1 and assign it to the root logical system LSYS0.

```
[edit system security-profile]
user@host#set p1 logical-system LSYS0
```

3. Configure a user logical system.

Step-by-Step Procedure

a. Create the user logical system LSYS1

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

b. Configure user logical and logical tunnel interfaces to transfer traffic within the logical system.

```
[edit interfaces]
user@host#set ge-0/0/0 unit 0 family inet address 198.51.100.0/24
user@host#set ge-0/0/1 unit 0 family inet address 203.0.113.0/24
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 10.0.0.0/8
```

c. Assign a security profile p1 to LSYS1.

```
[edit system security-profile]
user@host#set p1 logical-system LSYS1
```

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

```
[edit security zones]
user@host#set security-zone LSYS1_tzone host-inbound-traffic system-services all
user@host#set security-zone LSYS1_tzone host-inbound-traffic protocol all
user@host#set security-zone LSYS1_tzone interfaces ge-0/0/0
user@host#set security-zone LSYS1_utzone host-inbound-traffic system-services all
user@host#set security-zone LSYS1_utzone host-inbound-traffic protocol all
user@host#set security-zone LSYS1_utzone interfaces ge-0/0/1
```

4. Configure a security policy that permits FTP traffic from the LSYS1_tzone to LSYS1_utzone.

```
[edit security policies]
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 match source-address any
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 match destination-address
any
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 match application junos-
ftp
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 match application junos-
ping
user@host#set from-zone LSYS1_tzone to-zone LSYS1_utzone policy p11 then permit
user@host#set default-policy deny-all
```

Results

From configuration mode, confirm the configuration for LSYS0 and LSYS1 by entering the `show logical-systems`. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
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;
        }
    }
}
routing-instances {
    vr0 {
        instance-type vpls;
        interface lt-0/0/0.0;
        interface lt-0/0/0.2;
    }
}
```

```
user@host#show logical-systems LSYS1
interfaces {
    lt-0/0/0 {
        unit 1 {
            encapsulation ethernet;
            peer-unit 0;
            family inet {
                address 10.0.1.1/24;
            }
        }
    }
    reth0 {
        unit 0 {
            family inet {
```

```
                address 198.51.100.0/24;
            }
        }
    }
}
security {
    alg{
        ftp;
    }
    policies {
        from-zone LSYS1_tzone to-zone LSYS1_utzone {
            policy P11 {
                match {
                    source-address any;
                    destination-address any;
                    application [ junos-ping junos-ftp ];
                }
                then {
                    permit;
                }
            }
        }
        default-policy {
            deny-all;
        }
    }
    zones {
        security-zone LSYS1_tzone {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                reth0.0;
            }
        }
        security-zone LSYS1_utzone {
            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.

Verification

IN THIS SECTION

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

Verify ALG status for user logical system

Purpose

Verify alg status for FTP is enabled.

Action

To verify the configuration is working properly, enter the `show security alg status logical-system LSYS1` command.

```
user@host> show security alg status logical-system LSYS1
ALG Status:
```

```
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled
```

Meaning

The output displays the alg status for FTP Enabled for the logical system LSYS1.

Verify ALG status for all the logical systems

Purpose

Verify the ALG status for all the logical systems on the device.

Action

To verify the configuration is working properly, enter the `show security alg status logical-system all` command.

```
user@host> show security alg status logical-system all
Logical system: root-logical-system
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
```

```
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Disabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled

Logical system: LSYS3
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled

Logical system: LSYS1
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Disabled
```

```
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled

Logical system: LSYS2
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled

Logical system: LSYS0
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Disabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

```
   TWAMP    : Disabled
```

Meaning

The output displays the ALG status for all the logical systems on the device.

Verifying Intra-Logical System Traffic on a Logical System

Purpose

Verify the information about active resources, clients, groups, and sessions created through the resource manager.

Action

From operational mode, enter the `show security resource-manager summary` command.

```
 user@host> show security resource-manager summary
Active resource-manager clients   : 16
Active resource-manager groups    : 3
Active resource-manager resources : 26
Active resource-manager sessions  : 4
```

Meaning

The output displays summary information about active resources, clients, groups, and sessions created through the resource manager.

SEE ALSO

> Understanding Application Layer Gateway (ALG) in Logical Systems | **301**
>
> *show security alg status logical-system*

RELATED DOCUMENTATION

> Security Zones in Logical Systems | **145**

DHCP for Logical Systems

IN THIS SECTION

Understanding DHCP Support for Logical Systems

Starting in Junos OS Release 18.4R1, a logical system supports the DHCP client feature to learn IP addresses for interfaces assigned to the logical systems. Additionally, starting in Junos OS Release 18.4R1, logical systems support the DHCP relay feature. A DHCP relay agent forwards DHCP requests and responses between the DHCP client and the DHCP server.

A DHCP server allocates IP addresses and provides IP configuration settings such as the DNS server and default gateway to client hosts on a subnet served by an interface of a logical system. The DHCP allows network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network within a logical system. An IP address is leased to a host for a limited time period, allowing the DHCP server to share a limited IP addresses among a group of hosts that do not require permanent IP addresses.

An interface of an SRX Series Firewall operating as a DHCP client receives the TCP or IP settings and the IP address from an external DHCP server.

An SRX Series Firewall operating as a DHCP relay agent for logical systems forwards incoming requests from the DHCP clients to a specified DHCP server. The client requests pass through interfaces on the logical systems.

Minimum DHCPv6 Relay Agent Configuration for Logical Systems

The following example describes the minimum configuration required to configure an SRX Series Firewall as a DHCPv6 relay agent for the logical system.

Before you begin determine the following:

- The DHCPv6 relay group and the DHCP active server-group for logical system.

1. Configure an interface with an IPv6 address for the logical system.

```
user@host# set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 address
2001:db8::1/64
```

2. Specify the name of the server-group and add the IP address for the DHCP servers belonging to the same group.

```
user@host# set logical-systems LSYS1 forwarding-options dhcp-relay dhcpv6 group inf interface
ge-0/0/0.0
```

3. Specify the name of the active server group.

```
user@host# set logical-systems LSYS1 forwarding-options dhcp-relay dhcpv6 active-server-group
server6
```

4. Create a DHCP relay group that includes at least one interface for the logical system.

```
user@host# set logical-systems LSYS1 forwarding-options dhcp-relay dhcpv6 server-group
server6 2001:db8::1/64
```

5. Confirm your configuration by entering the `show logical-systems LSYS1` command.

```
[edit]
user@host# show logical-systems LSYS1
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet6 {
                address 2001:db8::1/64;;
            }
        }
    }
}
forwarding-options {
    dhcp-relay {
```

```
        dhcpv6 {
            group inf {
                interface ge-0/0/0.0;
            }
            server-group {
                server6 {
                    2001:db8::1/64;
                }
            }
            active-server-group server6;
        }
    }
}
```

NOTE: To configure the DHCP relay agent in a routing instance for the logical system, configure the `dhcp-relay` statement in the `edit logical-systems LSYS1 routing-instances R1` hierarchy level.

Example: Configuring the DHCPv6 Client for Logical Systems

IN THIS SECTION

This example shows how to configure an SRX Series Firewall as a DHCPv6 client for the logical systems.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall
- Junos OS Release 18.4R1

Before you begin:

- Read the Understanding DHCP Support for Logical Systems to understand how and where this procedure fits in the overall support for DHCP.

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

Overview

In this example, the primary administrator configures an SRX Series Firewall as a DHCPv6 client for a logical system.

The DHCPv6 client for a logical system includes the following features:

- Identity association for non-temporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Autoconfig or stateful mode
- DHCP unique identifier (DUID)

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic system-
services all
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic protocols all
set logical-systems LSYS1 security zones security-zone trust interfaces ge-0/0/0.0
```

```
set logical-systems LSYS1 routing-instances r1 instance-type virtual-router
set logical-systems LSYS1 routing-instances r1 interface ge-0/0/0.0
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type
autoconfig
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type
stateful
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type
ia-na
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type
ia-pd
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-
identifier duid-type duid-ll
set logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-
server
set protocols router-advertisement interface ge-0/0/0.0
```

Configuring DHCPv6 Client in a Logical System

Procedure

Step-by-Step Procedure

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

1. Configure the security zones to permit traffic for a logical system.

```
[edit logical-systems LSYS1 security zones]
user@host# set security-zone trust host-inbound-traffic system-services all
user@host# set security-zone trust host-inbound-traffic protocols all
user@host# set security-zone trust interfaces ge-0/0/0.0
```

2. Create a routing instance and assign the routing instance type for a logical system.

```
[edit logical-systems LSYS1]
user@host# set routing-instances r1 instance-type virtual-router
```

3. Specify the interface name for the routing instance.

```
[edit logical-systems LSYS1]
user@host# set routing-instances r1 interface ge-0/0/0.0
```

4. Configure the DHCPv6 client type. The client type can be `autoconfig` or `stateful` for the logical system.

   - To enable the DHCPv6 auto configuration mode, configure the client type as `autoconfig`.

```
[edit logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

   - For stateful address assignment, configure the client type as `stateful`.

```
[edit logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type stateful
```

5. Specify the identity association type.

   - To configure identity association for nontemporary address (IA_NA) assignment, specify the `client-ia type` as `ia-na`.

```
[edit logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

   - To configure identity association for prefix delegation (IA_PD), specify the `client-ia-type` as `ia-pd`.

```
[edit logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

6. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type for the logical system. The following DUID type is supported:

   - Link layer address (duid-ll)

```
[edit tlogical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

7. Specify the DHCPv6 client requested option as `dns-server` for the logical system.

```
[edit logical-systems LSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set req-option dns-server
```

8. Configure the router advertisement.

```
[edit]
user@host# set protocols router-advertisement interface ge-0/0/0.0
```

Results

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1` 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 LSYS1
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet6 {
                dhcpv6-client {
                    client-type stateful;
                    client-ia-type ia-na;
                    client-ia-type ia-pd;
                    client-identifier duid-type duid-ll;
                    req-option dns-server;
                }
            }
        }
    }
}
routing-instances {
    r1 {
        instance-type virtual-router;
        interface ge-0/0/0.0;
    }
}
security {
    zones {
```

```
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
    }
}
```

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

```
user@host# show protocols
router-advertisement {
    interface ge-0/0/0.0;
}
```

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

Verification

IN THIS SECTION

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

Verifying the DHCPv6 Client for Logical Systems

Purpose

Verify that the DHCPv6 client information is configured.

Action

From the operational mode, enter the `show dhcpv6 client binding logical-systems LSYS1` command.

```
user@host> show dhcpv6 client binding  logical-systems LSYS1
 IP/prefix                       Expires     State      ClientType    Interface       Client DUID
        2000::17/128                    67762       BOUND      STATEFUL      ge-0/0/6.0
LL0x3-10:0e:7e:49:25:86
        2000:100::/64                   67762       BOUND      STATEFUL      ge-0/0/6.0
LL0x3-10:0e:7e:49:25:86
```

Meaning

The output displays the address binding information for the logical system.

Verifying the DHCPv6 Client Binding for Logical Systems

Purpose

Verify that the DHCPv6 client binding information is configured.

Action

From the operational mode, enter the `show dhcpv6 client binding detail logical-systems LSYS1` command.

```
user@host> show dhcpv6 client binding detail logical-systems LSYS1
Client Interface/Id: ge-0/0/6.0
     Hardware Address:             10:0e:7e:49:25:86
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
     ClientType:                   STATEFUL
     Lease Expires:                2018-11-09 07:11:47 UTC
     Lease Expires in:             67760 seconds
     Lease Start:                  2018-11-08 07:11:47 UTC
```

```
     Bind Type:                    IA_NA IA_PD
     Preferred prefix length       0
     Sub prefix length             0
     Client DUID:                  LL0x3-10:0e:7e:49:25:86
     Rapid Commit:                 Off
     Server Identifier:            fe80::46f4:77ff:fed6:670a
     Client IP Address:            2000::17/128
     Client IP Prefix:             2000:100::/64


     DHCP options:
    Name: server-identifier, Value: VENDOR0x00000583-0x34343a34
```

Meaning

The output displays the detailed client binding information for the logical system.

Verifying the DHCPv6 Client Statistics for Logical Systems

Purpose

Verify that the DHCPv6 client statistics information is configured.

Action

From the operational mode, enter the `show dhcpv6 client statistics logical-systems LSYS1` command.

```
user@host> show dhcpv6 client statistics logical-systems LSYS1
Dhcpv6 Packets dropped:
     Total               3
     Bad Send            3

    Messages received:
    DHCPV6_ADVERTISE           1
    DHCPV6_REPLY               1
    DHCPV6_RECONFIGURE         0

    Messages sent:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             1
```

```
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             1
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
```

Meaning

The output displays the information about the number of packets discarded, the number of messages received and the number of messages sent by the DHCP client for the logical system.

Example: Configuring the DHCPv6 Server Options for Logical Systems

IN THIS SECTION

This example shows how to configure DHCPv6 server options on SRX Series Firewalls for the logical system.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall
- Junos OS Release 18.4R1

Before you begin determine the following:

- The IPv6 address pool range and the IPv6 prefix for logical systems.

Overview

In this example, you set a default client limit as 200 for all DHCPv6 groups. You then create a group called `my-group` that contains at least one interface. In this case, the interface is ge-0/0/2.0. You set a range of interfaces using the `upto` command and set a custom client limit as 200 for group `my-group` that overrides the default limit. Finally, you configure interface ge-0/0/2.0 with IPv6 address 2001:db8::1/64 and set router advertisement for interface ge-0/0/2.0.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems LSYS1 system services dhcp-local-server dhcpv6 group my-group overrides
interface-client-limit 200
set logical-systems LSYS1 system services dhcp-local-server dhcpv6 group my-group interface
ge-0/0/2.0
set logical-systems LSYS1 interfaces ge-0/0/2 unit 0 family inet6 address 2001:db8::1/64
set logical-systems LSYS1 access address-assignment pool my-pool family inet6 prefix
2001:db8::1/64
set logical-systems LSYS1 access address-assignment pool my-pool family inet6 range r1 low
2001:db8::1/64
set logical-systems LSYS1 access address-assignment pool my-pool family inet6 range r1 high
2001:db8::1/64
set logical-systems LSYS1 access address-assignment pool my-pool family inet6 dhcp-attributes
maximum-lease-time 200
set logical-systems LSYS1 access address-assignment pool my-pool family inet6 dhcp-attributes
option 21 string sip1.net
```

```
set logical-systems LSYS1 protocols router-advertisement interface ge-0/0/2.0 prefix
2001:db8::1/64
```

Procedure

Step-by-Step Procedure

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

To configure the DHCPv6 server options for logical systems:

1. Configure a DHCP local server.

```
[edit logical-systems LSYS1]
user@host# set system services dhcp-local-server dhcpv6
```

2. Set a default limit for all DHCPv6 groups.

```
[edit logical-systems LSYS1 system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

3. Specify a group name and interface.

```
[edit logical-systems LSYS1 system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/2.0
```

4. Configure an interface with an IPv6 address.

```
[edit logical-systems LSYS1 interfaces]
user@host# set ge-0/0/2 unit 0 family inet6 address 2001:db8::1/64
```

5. Configure an address-pool and specify the IPv6 family.

```
[edit logical-systems LSYS1 access]
user@host# set address-assignment pool my-pool family inet6 prefix 2001:db8::1/64
```

6. Configure the IPv6 prefix, the range name, and the IPv6 range for the DHCPv6 clients

```
[edit logical-systems LSYS1 access]
user@host# set address-assignment pool my-pool family inet6 range r1 low 2001:db8::1/64
user@host# set address-assignment pool my-pool family inet6 range r1 high 2001:db8::1/64
```

7. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit logical-systems LSYS1 access]
user@host# set address-assignment pool my-pool family inet6 dhcp-attributes maximum-lease-
time 200
```

8. Configure the user-defined option.

```
[edit logical-systems LSYS1 access]
user@host# set address-assignment pool my-pool family inet6 dhcp-attributes option 21 string
sip1.net
```

9. Configure the router advertisement for the interface.

```
[edit logical-systems LSYS1 protocols]
user@host# set router-advertisement interface ge-0/0/2.0 prefix 2001:db8::1/64
```

Results

From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1` 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 LSYS1
interfaces {
    ge-0/0/2 {
        unit 0 {
            family inet6 {
                address 2001:db8::1/64;
            }
        }
    }
```

```
}
protocols {
    router-advertisement {
        interface ge-0/0/2.0 {
            prefix 2001:db8::1/64;
        }
    }
}
system {
    services {
        dhcp-local-server {
            dhcpv6 {
                group my-group {
                    overrides {
                        interface-client-limit 200;
                    }
                    interface ge-0/0/2.0;
                }
            }
        }
    }
}
access {
    address-assignment {
        pool my-pool {
            family inet6 {
                prefix 2001:db8::1/64;
                range r1 {
                    low 2001:db8::1/64;
                    high 2001:db8::1/64;
                }
                dhcp-attributes {
                    maximum-lease-time 200;
                    option 21 string sip1.net;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the DHCPv6 Local Server Configuration

Purpose

Displays the address bindings in the client table on the extended DHCPv6 local server.

Action

From operational mode, enter the `show dhcpv6 server binding summary` command to display the address bindings in the client table on the DHCPv6 local server.

```
user@host> show dhcpv6 server binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

Meaning

The output displays the information about the DHCPv6 local server address binding summary.

Application Security in Logical Systems

IN THIS SECTION

Application Security in logical systems enables to identify application traffic traversing your network regardless of port, protocol, and encryption, thereby providing greater visibility to control network traffic. The application security controls network traffic by setting and enforcing security policies based on accurate application information. For more information, see the following topics:

Understanding Logical Systems 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 primary 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.

Starting in Junos OS Release 18.2R1, the default behavior of the ASC is changed as follows:

- Security services including security policies, application firewall (AppFW), application tracking (AppTrack), application quality of service (AppQoS), Juniper ATP Cloud, IDP, and Content Security do not use the ASC by default.
- Miscellaneous services including advanced policy-based routing (APBR) use the ASC for application identification by default.

  For more information, see *Enabling or Disabling Application System Cache for Application Services*.

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

Application signature package is installed at the global-level, that is shared by all user logical systems. The primary logical system administrator can install or uninstall application signature package.

Starting in Junos OS Release 18.3R1, the application identification (AppID) support for logical systems include two new options to view and clear logical system statistics and logical system counters statistics.

The primary logical system administrator can display or clear the statistics for all logical systems whereas the administrator for the user logical system can display or clear the statistics for their own logical system.

The user logical system administrator can view the AppID signature package status and version. Custom signatures configured by the primary logical system administrator can be configured in the use logical system security policies.

You can view the status and version information about the AppID signature package status and version by using the commands `show services application-identification status` and `show services application-identification version`.

SEE ALSO

- Understanding the Junos OS Application Identification Database
- Example: Scheduling the Application Signature Package Updates
- Example: Configuring Junos OS Application Identification Custom Application Signatures
- Understanding IDP Application Identification
- Understanding the Application System Cache
- Verifying Application System Cache Statistics

Understanding Logical Systems 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 primary administrator can download a predefined application signature database from the Juniper Networks Security Engineering website or can define application signatures using the Junos OS configuration CLI. For more information about application identification and application signatures, see Application Security User Guide for Security Devices.

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 primary administrator can configure, enable, and monitor application firewalls on the primary 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.

SEE ALSO

Example: Configuring Application Firewall Services for a Primary Logical Systems | 338

Example: Configuring Application Firewall Services for a User Logical System | 345

Example: Configuring Application Firewall Services for a Primary Logical Systems

IN THIS SECTION

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

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

For information about configuring an application firewall within a security policy, see *Application Firewall Overview*.

Requirements

Before you begin:

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

  See "Example: Configuring Security Features for the Primary Logical Systems" on page 172.

- Verify that application firewall resources (appfw-rule-set and appfw-rule) have been allocated in a security profile and bound to the primary 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 primary administrator allocates various global system resources through a security profile configuration which is then bound to the various logical systems on the device. The primary administrator owns this function and configures the security profile for all user logical systems as well as the primary logical system.

For more information, see "Understanding Logical Systems Security Profiles (Primary Administrators Only)" on page 68.

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

  For information about primary administrator role functions, see "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

Overview

IN THIS SECTION

In this example you create application firewall services on the primary logical system, called root-logical-system shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54.

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, example2 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.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set 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

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 application firewall for a primary logical system:

1. Log in to the primary logical system as the primary administrator. See "Example: Configuring Root Password for Logical Systems" on page 52 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

IN THIS SECTION

- Verifying Application Firewall Configuration | 343

Confirm that the configuration is working properly.

Verifying Application Firewall Configuration

Purpose

View the application firewall configuration on the primary 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
```

SEE ALSO

- SRX Series Logical Systems Primary Administrator Configuration Tasks Overview | 22
- Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68
- Understanding Logical Systems Application Firewall Services | 337
- Example: Configuring Security Features for the Primary Logical Systems | 172

Understanding Logical Systems 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 primary 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 in to.

NOTE: The system log configuration is global on the device and must be configured by the primary 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 primary administrator as well as user logical system administrators can view AppTrack counters with the `show security application-tracking counters` command.

SEE ALSO

- Understanding AppTrack

Example: Configuring Application Firewall Services for a User Logical System

IN THIS SECTION

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

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

For information about configuring an application firewall within a security policy, see *Application Firewall Overview*.

Requirements

Before you begin:

- Verify that the security zones are configured for the user logical system.
- Verify that the primary 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 (Primary Administrators Only)" on page 68.
- 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 50.

Overview

IN THIS SECTION

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 54.

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.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security 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

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 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

IN THIS SECTION

- Verifying Application Firewall Configuration | 350

Confirm that the configuration is working properly.

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
```

SEE ALSO

User Logical Systems Configuration Overview | 48

Understanding Logical Systems Application Firewall Services | 337

Example: Configuring AppTrack for a User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- (Primary administrator) Configure system logging in the primary logical system. See Network Management and Monitoring Guide.

Overview

IN THIS SECTION

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 54.

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.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

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

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 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

IN THIS SECTION

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

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.

SEE ALSO

Understanding Logical Systems Application Tracking Services | 344

User Logical Systems Configuration Overview | 48

IPv6 for Logical Systems

IN THIS SECTION

IPv6 builds upon the functionality of IPv4, providing improvements to IP addressing, configuration and maintenance, and security. IPv6 supports extensions for authentication and data integrity, which enhance privacy and security. IPv6 uses 128-bit addresses and supports a virtually unlimited number of devices—2 to the 128th power. For more information, see the following topics:

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 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.

SEE ALSO

Understanding IPv6 Address Space, Addressing, Address Format, and Address Types

Example: Configuring IPv6 for the Primary, Interconnect, and User Logical Systems (Primary Administrators Only) | **358**

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) (Primary Administrators Only) | **451**

Understanding IPv6 Dual-Stack Lite in Logical Systems | **357**

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 primary 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 primary administrator can configure a security profile for the primary logical system that specifies the maximum and reserved numbers of softwire initiators that can connect to a softwire concentrator configured for the primary logical system. The number of softwire initiators configured in the primary 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 primary administrator can configure softwire concentrators for the primary logical system at the

[edit security softwires] hierarchy level. The primary 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.

SEE ALSO

- Example: Configuring IPv6 Dual-Stack Lite for a User Logical Systems | 379
- Understanding Logical Systems Security Profiles (Primary Administrators Only) | 68
- *Understanding IPv6 Dual-Stack Lite*

Example: Configuring IPv6 for the Primary, Interconnect, and User Logical Systems (Primary Administrators Only)

IN THIS SECTION

This topic covers configuration of IPv6 interfaces, static routes, and routing instances for the primary 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 Systems Primary Administrator Configuration Tasks Overview" on page 22 to understand how and where this procedure fits in the overall primary administrator configuration process.

- See "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54.
- See "Understanding the Interconnect Logical System and Logical Tunnel Interfaces" on page 9.

Overview

IN THIS SECTION

- Topology | 360

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 primary 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 primary 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 9 on page 360 shows the topology for this deployment including virtual routers and their interfaces for all IPv6 logical systems.

Topology

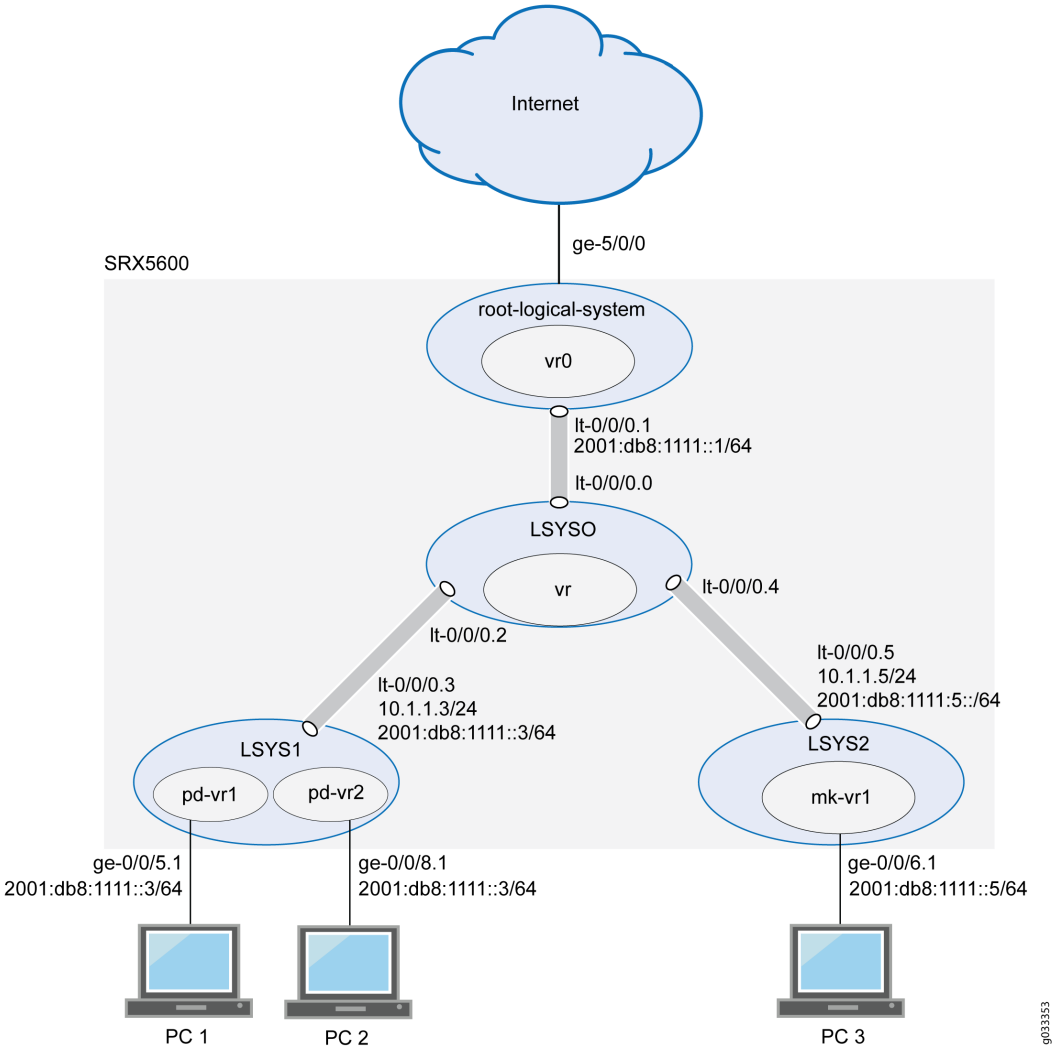


Figure 9: Configuring IPv6 Logical Tunnel Interfaces, Logical Interfaces, and Virtual Routers

Configuration

IN THIS SECTION

This topic explains how to configure interfaces for logical systems.

Configuring Logical Tunnel Interfaces and a Routing Instance for the Interconnect Logical System

CLI Quick Configuration

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

```
set 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 Primary Logical System

CLI Quick Configuration

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

```
set interfaces ge-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 10.1.1.1/24
set interfaces lt-0/0/0 unit 1 family inet6 address 2001:db8:1111::1/64
set interfaces ge-5/0/0 unit 0 family inet address 10.99.99.1/24
set interfaces ge-5/0/0 unit 0 family inet6 address 2001:db8:9999::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 2001:db8:777::/64 next-hop
2001:db8:1111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 2001:db8:888::/64 next-hop
2001:db8:1111::3
set routing-instances vr0 routing-options rib vr0.inet6.0 static route 2001:db8:666::/64 next-hop
2001:db8:1111::5
set routing-instances vr0 routing-options static route 192.168.7.0/24 next-hop 10.1.1.3
```

```
set routing-instances vr0 routing-options static route 192.168.8.0/24 next-hop 10.1.1.3
set routing-instances vr0 routing-options static route 192.168.6.0/24 next-hop 10.1.1.5
```

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*.

To configure the primary logical system interfaces:

1. Configure the primary (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 10.1.1.1/24
user@host# set lt-0/0/0 unit 1 family inet6 address 2001:db8:1111::1/64
user@host# set ge-5/0/0 unit 0 family inet address 10.99.99.1/24
user@host# set ge-5/0/0 unit 0 family inet6 address 2001:db8:9999::1/64
```

2. Configure a routing instance for the primary 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 2001:db8:1111:777/64 next-hop
2001:db8:1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 2001:db8:1111:888/64 next-hop
2001:db8:1111::3
user@host# set vr0 routing-options rib vr0.inet6.0 static route 2001:db8:1111:666/64 next-hop
2001:db8:1111::5
user@host# set vr0 routing-options static route 192.168.7.0/24 next-hop 10.1.1.3
user@host# set vr0 routing-options static route 192.168.8.0/24 next-hop 10.1.1.3
user@host# set vr0 routing-options static route 192.168.6.0/24 next-hop 10.1.1.5
```

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 10.99.99.1/24;
        }
        family inet 6{
            address 2001:db8:9999:1/64;
        }
    }
}
lt-0/0/0 {
    unit 1 {
        encapsulation ethernet;
        peer-unit 0;
        family inet {
            address 10.1.1.1/24;
        }
        family inet 6{
            address 2001:db8:1111::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 2001:db8:1111:888/64 next-hop 2001:db8:1111:3;
            route 2001:db8:1111:777/64 next-hop 2001:db8:1111:3;
            route 2001:db8:1111:666/64 next-hop 2001:db8:1111:5;
        }
        }
        static {
            route 192.168.7.0/24 next-hop 10.1.1.3;
            route 192.168.8.0/24 next-hop 10.1.1.3;
            route 192.168.6.0/24 next-hop 10.1.1.5;
        }
    }
}
```

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

```
set 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 10.1.1.3/24
set logical-systems LSYS1 interfaces lt-0/0/0 unit 3 family inet6 address 2001:db8:1111:2/64
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 10.1.1.5/24
set logical-systems LSYS2 interfaces lt-0/0/0 unit 5 family inet6 address 2001:db8:1111::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*.

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 10.1.1.3/24
user@host# set family inet6 address 2001:db8:1111:3::1/64
```

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 10.1.1.5/24
user@host# set family inet6 address 2001:db8:1111::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 10.1.1.3/24;
        }
        family inet 6{
            address 2001:db8:1111::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 10.1.1.5/24;
        }
        family inet 6{
            address 2001:db8:1111::5/64;
        }
    }
}
```

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

Verification

IN THIS SECTION

- Verifying That the Static Routes Configured for the Primary Administrator Are Correct | 368

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

Purpose

Confirm that the configuration is working properly. Verify if you can send data from the primary logical system to the other logical systems.

Action

From operational mode, use the `ping` command.

SEE ALSO

Understanding the Primary Logical Systems and the Primary Administrator Role | 21

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Understanding the Interconnect Logical System and Logical Tunnel Interfaces | 9

Example: Configuring IPv6 Zones for a User Logical Systems | 369

Example: Configuring IPv6 Security Policies for a User Logical Systems | 374

Example: Configuring IPv6 Zones for a User Logical Systems

IN THIS SECTION

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 Systems Configuration Overview" on page 48.

- 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 54

This example creates the IPv6 zones and address books described in Table 24 on page 370.

Table 24: 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

IN THIS SECTION

- Procedure | 371

Procedure

CLI Quick Configuration

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

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

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.

SEE ALSO

- Understanding Logical Systems Zones | 145
- User Logical Systems Configuration Overview | 48
- Example: Configuring IPv6 for the Primary, Interconnect, and User Logical Systems (Primary Administrators Only) | 358
- Example: Configuring IPv6 Security Policies for a User Logical Systems | 374

Example: Configuring IPv6 Security Policies for a User Logical Systems

IN THIS SECTION

This example shows how to configure IPv6 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 Systems Configuration Overview" on page 48.

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

  See "Example: Configuring IPv6 Zones for a User Logical Systems" on page 369

Overview

This example shows how to configure the security policies described in Table 25 on page 375.

Table 25: 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

IN THIS SECTION

- Procedure | 376

Procedure

CLI Quick Configuration

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

```
set 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

IN THIS SECTION

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.

SEE ALSO

- Understanding Logical Systems Security Policies | 210
- User Logical Systems Configuration Overview | 48
- Troubleshooting Security Policies
- Example: Configuring IPv6 Zones for a User Logical Systems | 369
- Example: Configuring IPv6 for the Primary, Interconnect, and User Logical Systems (Primary Administrators Only) | 358

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

IN THIS SECTION

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 Systems Configuration Overview" on page 48.
- Use the `show system security-profile dslite-softwire-initiator` command to see the number softwire initiators that can be connected to a softwire concentrator in the logical system.

Overview

This example shows how to configure a softwire concentrator to decapsulate IPv4-in-IPv6 packets in the ls-product-design user logical system shown in "Example: Creating User Logical Systems, Their Administrators, Their Users, and an Interconnect Logical System" on page 54. The IPv6 address of the softwire concentrator is 3000::1 and the name of the softwire configuration is sc_1.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security 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

IN THIS SECTION

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
```

SEE ALSO

- Understanding IPv6 Dual-Stack Lite in Logical Systems | 357
- User Logical Systems Configuration Overview | 48

RELATED DOCUMENTATION

- Understanding Logical Systems Zones | 145

SSL Proxy for Logical Systems

IN THIS SECTION

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. For more information, see the following topics:

Understanding SSL Forward and Reverse Proxy for Logical Systems

SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. SSL, also called Transport Layer Security (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity.

SSL proxy is a transparent proxy that performs SSL encryption and decryption between the client and the server as follows:

- Reverse proxy is an inbound session, that is, externally initiated SSL sessions from the Internet to the local server.

  The proxy model implementation for server protection (often called reverse proxy) is supported on SRX Series Firewalls to provide improved handshaking and support for more protocol versions.

- Forward proxy is an outbound session, that is, locally initiated SSL session to the Internet.

SSL proxy works transparently between the client and the server. All requests from a client first go to the proxy server; the proxy server evaluates the request, and if the request is valid, forwards the request to the outbound side. Similarly, inbound requests are also evaluated by the proxy server. Both client and server interpret that they are communicating with each other; however, it is the SSL proxy that functions between the two.

Example: Configuring SSL Forward and Reverse Proxy for Logical Systems

IN THIS SECTION

This example shows how to configure SSL proxy to enable server protection. A reverse proxy protects servers by hiding the details of the servers from the clients, there by adding an extra layer of security and the purpose of a forward proxy is to manage traffic to the client systems.

Requirements

To configure an SSL reverse and forward proxy, you must:

- Load the server certificates and their keys into SRX Series Firewall's certificate repository.
- Attach the server certificate identifiers to the SSL proxy profile.
- Apply SSL proxy profile as application services in a security policy.

Overview

This example shows how to configure reverse proxy to enable server protection and forward proxy is for client protection. It shows how to configure an SSL proxy profile and apply it at the security policy rule level. For server protection, additionally, server certificates with private keys must be configured.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems LSYS1 services ssl proxy profile ssl-fp-profile root-ca new-srvr-cert
set logical-systems LSYS1 services ssl proxy profile ssl-fp-profile actions ignore-server-auth-
failure
set logical-systems LSYS1 services ssl proxy profile ssl-rp-profile actions log all
set logical-systems LSYS1 security log mode event
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 match
source-address any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 match
destination-address any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 match
application any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 then permit
application-services ssl-proxy profile-name ssl-rp-profile
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 then log
session-init
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy 1 then log
session-close
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 match
source-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 match
destination-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 match
application any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 then permit
application-services ssl-proxy profile-name ssl-rp-profile
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 then log
session-init
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy 1 then log
session-close
```

Configuring the SSL Reverse and Forward Proxy

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 SSL Proxy:

1. Configure the SSL Reverse Proxy.

```
[edit logical-systems LSYS1]
user@host# set logical-systems LSYS1 services ssl proxy profile ssl-rp-profile  actions log
all
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 match source-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 match destination-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 match application any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 then permit application-services ssl-proxy profile-name ssl-rp-profile
```

2. Configure the SSL Forward Proxy.

```
[edit logical-systems LSYS1]
user@host# set logical-systems LSYS1 services ssl proxy profile ssl-fp-profile  root-ca new-
srvr-cert
user@host# set logical-systems LSYS1 services ssl proxy profile ssl-fp-profile  actions
ignore-server-auth-failure
user@host# set logical-systems LSYS1 security log mode event
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 match source-address any
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 match destination-address any
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 match application any
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 then permit application-services idp
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 then permit application-services ssl-proxy profile-name ssl-rp-profile
```

```
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 then log session-init
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy
1 then log session-close
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 then log session-init
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
1 then log session-close
```

Results

From configuration mode, confirm your configuration by entering the `show logical-system LSYS1 services ssl proxy` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

You must configure either `root-ca` (forward proxy) or `server-certificate` (reverse proxy) in an SSL proxy profile. Otherwise, the commit check fails.

```
user@host# show logical-systems LSYS1 services ssl proxy
profile ssl-rp-profile {
    server-certificate ssl-inspect-sp1;  { # For reverse proxy. No root-ca is needed.
    actions {
        log {
            all;
        }
    }
}
profile ssl-fp-profile { # For forward proxy. No server cert/key is needed.
    root-ca new-srvr-cert;
    actions {
        ignore-server-auth-failure;
        log {
            all;
        }
    }
}
```

Verification

IN THIS SECTION

Verifying the SSL Proxy Configuration on the Device

Purpose

Viewing the SSL reverse proxy statistics on the SRX Series Firewall.

Action

You can view the SSL proxy statistics by using the `show services ssl proxy statistics logical-system` command.

```
user@host> show services ssl proxy statistics logical-system LSYS1
PIC:spu-3 fpc[0] pic[3] ------
        sessions matched                                1
        sessions bypassed:non-ssl                       0
        sessions bypassed:mem overflow                  0
        sessions bypassed:low memory                    0
        sessions created                                1
        sessions ignored                                0
        sessions active                                 1
        sessions dropped                                0
        sessions whitelisted                            0
        whitelisted url category match                  0
        default profile hit                             0
        session dropped no default profile              0
        policy hit no profile configured                0
```

SEE ALSO

- Example: Loading CA and Local Certificates Manually
- Example: Configuring a Device for Peer Certificate Chain Validation

ICAP Redirects for Logical Systems

IN THIS SECTION

ICAP is a lightweight protocol used to extend transparent proxy servers, thereby freeing up resources. For more information, see the following topics:

ICAP Redirect Support for Logical Systems

IN THIS SECTION

Starting in Junos OS Release 18.3R1, SRX Series Firewalls support the Internet Content Adaptation Protocol (ICAP) service redirect when the device is configured for logical systems.

ICAP redirect profile is only allowed to attach on the policy which belongs to the same logical system. This profile is applied to a security policy as application services for the permitted traffic. The ICAP profile defines the settings that allow the ICAP server to process request messages, response messages, fallback options (in case of a timeout), connectivity issues, too many requests, or any other conditions.

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. SSL, also called Transport Layer Security (TLS), ensures the secure transmission of

data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private-public key exchange pairs for this level of security. SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence.

ICAP redirect services has the dependency on SSL proxy to build secure connections. Because the SSL proxy is not supported on user logical systems in Junos OS Release 18.3R1, ICAP redirect works with clear text connections or with shared certificates in Junos OS Release 18.3R1.

The following sequences are involved in a typical ICAP redirect scenario:

1. The user opens a connection to a Website on the internet.
2. The request goes through the SRX Series Firewall that is acting as a proxy server.
3. The SRX Series Firewall receives information from the end-host, encapsulates the message and forwards the encapsulated ICAP message to the third-party on-premise ICAP server.
4. The ICAP server receives the ICAP request and analyzes it.
5. If the request does not contain any confidential information, the ICAP server sends it back to the proxy server, and directs the proxy server to send the HTTP to the internet.
6. If the request contains confidential information, you can choose to take action (block, permit and log) as per your requirement.

Limitations of SSL Proxy with Logical Systems

Following are the limitations for using ICAP redirect service for user logical systems:

- SSL Proxy is supported only on primary logical system in Junos OS Release 18.3R1.
- SSL profile configured to provide a secure connection to the ICAP server is not supported on user logical systems in Junos OS Release 18.3R1.

SEE ALSO

SSL Proxy

Example: Configuring ICAP Redirect Service on SRX Series Firewalls

IN THIS SECTION

This example shows how to define an ICAP redirect profile for an SRX Series Firewall.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall with Junos OS Release 18.3R1 or later. This configuration example is tested for Junos OS Release 18.3R1.

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

Overview

In this example, you configure an ICAP redirect profile in logical systems and apply these profiles as application services in the security policy for the permitted traffic.

Table 26 on page 391 lists the details of the parameters used in this example.

Table 26: ICAP Redirect Configuration Parameters

Parameters	Names	Description
Profile	icap-pf1	The ICAP server profile allows the ICAP server to process request messages, response messages, fallback options and so on, for the permitted traffic. This profile is applied as an application service in the security policy.
Server name	icap-svr1 icap-svr2	The machine name of the remote ICAP host. Client's request is redirected to this ICAP server.

Table 26: ICAP Redirect Configuration Parameters *(Continued)*

Parameters	Names	Description
Server IP address	192.0.2.2/24 192.0.2.179/24	The IP address of the remote ICAP host. Client's request is redirected to this ICAP server.
Logical system name	LSYS1	Displays the logical system name which belongs to the same profile.
Security policy	sp1	In a security policy, apply the SSL proxy profile and ICAP redirect profile. to the permitted traffic.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 host
192.0.2.2/24
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri
echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 respmod-uri
echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr1 sockets 64
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 host
192.0.2.179/24
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri
```

```
echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 respmod-uri
echo
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 sockets 64
set logical-systems LSYS1 services icap-redirect profile icap-pf1 server icap-svr2 tls-profile
dlp_ssl
set logical-systems LSYS1 services icap-redirect profile icap-pf1 http redirect-request
set logical-systems LSYS1 services icap-redirect profile icap-pf1 http redirect-response
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy sec_policy
match source-address any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy sec_policy
match destination-address any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy sec_policy
match application any
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy sec_policy
then permit application-services ssl-proxy profile-name ssl-inspect-profile
set logical-systems LSYS1 security policies from-zone trust to-zone untrust policy sec_policy
then permit application-services icap-redirect icap-pf1
set logical-systems LSYS1 security policies default-policy permit-all
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic system-
services all
set logical-systems LSYS1 security zones security-zone trust host-inbound-traffic protocols all
set logical-systems LSYS1 security zones security-zone trust interfaces xe-5/0/0.0
set logical-systems LSYS1 security zones security-zone untrust host-inbound-traffic system-
services all
set logical-systems LSYS1 security zones security-zone untrust host-inbound-traffic protocols all
set logical-systems LSYS1 security zones security-zone untrust interfaces xe-5/0/1.0
set logical-systems LSYS1 interfaces xe-5/0/0 unit 0 family inet address 192.0.2.1/8
set logical-systems LSYS1 interfaces xe-5/0/0 unit 0 family inet6 address 2001:db8::1/64
set logical-systems LSYS1 interfaces xe-5/0/1 unit 0 family inet address 198.51.100.1/8
set logical-systems LSYS1 interfaces xe-5/0/1 unit 0 family inet6 address 2001:db8::2/64
```

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 CLI User Guide.

To configure the ICAP redirect service:

1. Configure the ICAP redirect profile for the first server (icap-svr1).

```
[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 server icap-svr1 host 192.0.2.2/24
user@host# set icap-redirect profile icap-pf1 server icap-svr1 reqmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr1 respmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr1 sockets 64
```

2. Configure the ICAP redirect profile for the second server (icap-svr2).

```
[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 server icap-svr2 host 192.0.2.179/24
user@host# set icap-redirect profile icap-pf1 server icap-svr2 reqmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 respmod-uri echo
user@host# set icap-redirect profile icap-pf1 server icap-svr2 sockets 64
user@host# set icap-redirect profile icap-pf1 server icap-svr2 tls-profile dlp_ssl
```

3. Configure the redirect request and the redirect response for the HTTP traffic.

```
[edit logical-systems LSYS1 services]
user@host# set icap-redirect profile icap-pf1 http redirect-request
user@host# set icap-redirect profile icap-pf1 http redirect-response
```

4. Configure a security policy to apply application services for the ICAP redirect to the permitted traffic.

```
[edit logical-systems LSYS1 security]
user@host# set policies from-zone trust to-zone untrust policy sec_policy match source-
address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match destination-
address any
user@host# set policies from-zone trust to-zone untrust policy sec_policy match application
any
user@host# set policies from-zone trust to-zone untrust policy sec_policy then permit
application-services ssl-proxy profile-name ssl-inspect-profile
user@host# set policies from-zone trust to-zone untrust policy sec_policy then permit
application-services icap-redirect icap-pf1
user@host# set policies default-policy permit-all
```

5. Configure zones.

```
[edit logical-systems LSYS1 security]
user@host# set zones security-zone trust host-inbound-traffic system-services all
user@host# set zones security-zone trust host-inbound-traffic protocols all
user@host# set zones security-zone trust interfaces xe-5/0/0.0
user@host# set zones security-zone untrust host-inbound-traffic system-services all
user@host# set zones security-zone untrust host-inbound-traffic protocols all
user@host# set zones security-zone untrust interfaces xe-5/0/1.0
```

6. Configure interfaces.

```
[edit logical-systems LSYS1]
user@host# set interfaces xe-5/0/0 unit 0 family inet address 192.0.2.1/8
user@host# set interfaces xe-5/0/0 unit 0 family inet6 address 2001:db8::1/64
user@host# set interfaces xe-5/0/1 unit 0 family inet address 198.51.100.1/8
user@host# set interfaces xe-5/0/1 unit 0 family inet6 address 2001:db8::2/64
```

Results

From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1 services icap-redirect`, `show logical-systems LSYS1 security policies`, `show logical-systems LSYS1 security zones`, and `show logical-systems LSYS1 interfaces` 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 LSYS1 services icap-redirect
profile icap-pf1 {
    server icap-svr1 {
        host 192.0.2.2/24;
        reqmod-uri echo;
        respmod-uri echo;
        sockets 64;
    }
    server icap-svr2 {
        host 192.0.2.179/24;
        reqmod-uri echo;
        respmod-uri echo;
        sockets 64;
        tls-profile dlp_ssl;
```

```
    }
    http {
        redirect-request;
        redirect-response;
    }
}
```

```
from-zone trust to-zone untrust {
    policy sec_policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    ssl-proxy {
                        profile-name ssl-inspect-profile;
                    }
                    icap-redirect icap-pf1;
                }
            }
        }
    }
}
default-policy {
    permit-all;
}
```

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

Verification

IN THIS SECTION

- Verifying ICAP Redirect Configuration | 397

Verifying ICAP Redirect Configuration

Purpose

Verify that the ICAP redirect service is configured on the device.

Action

From operational mode, enter the `show services icap-redirect status logical-system` and `show services icap-redirect statistic logical-system` commands.

```
user@host> show services icap-redirect status logical-system LSYS1

ICAP Status :
         spu-1 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
         spu-2 Profile: icap-pf1 Server: icap-svr1 : UP
ICAP Status :
         spu-3 Profile: icap-pf1 Server: icap-svr1 : UP

user@host> show services icap-redirect statistic logical-system LSYS1

ICAP Redirect statistic:
  Message Redirected                 : 12
      Message REQMOD Redirected      : 6
      Message RESPMOD Redirected     : 6
  Message Received                   : 12
      Message REQMOD Received        : 6
      Message RESPMOD Received       : 6
Fallback:      permit           log-permit       reject
  Timeout         0                0                0
  Connectivity    0                0                0
  Default         0                0                0
```

Meaning

The status `Up` indicates that the ICAP redirect service is enabled. The `Message Redirected` and the `Message Received` fields show the number of HTTP requests that have passed through the ICAP channel.

RELATED DOCUMENTATION

Example: Configuring Logical Systems Security Profiles (Primary Administrators Only) | 74

AppQoS for Logical Systems

IN THIS SECTION

Application quality of service (AppQoS) enable you to identify and control access to specific applications and provides the granularity of the stateful firewall rule base to match and enforce quality of service (QoS) at the application layer. AppQoS feature expands the capability of Junos OS class of service (CoS) for logical systems.

Application Quality of Service Support for Logical Systems Overview

The application quality of service (AppQoS) feature expands the capability of Junos OS class of service (CoS) for logical systems. This includes marking DSCP values based on Layer-7 application types, honoring application-based traffic through loss priority settings, and controlling transfer rates on egress PICs based on Layer-7 application types.

When a network experiences congestion and delay, some packets must be dropped. Junos OS CoS allows you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to the rules you configure.

Logical system enables you to partition a single device into multiple domains to perform security and routing functions.

Starting in Junos OS Release 19.3R1, AppQoS is supported when the SRX Series Firewall is configured with logical system. You can configure a default AppQoS rule set to manage the application- traffic-control within the logical system. AppQoS provides the ability to prioritize and meter the application traffic to provide better service to business-critical or high-priority application traffic.

AppQoS rule sets are included in the logical system to implement application-aware quality-of-service control. You can configure a rule set with rules under the application-traffic-control option, and attach the AppQoS rule set to a logical system as an application service. If the traffic matches the specified application the application-aware quality of service is applied for logical system.

For AppQoS, traffic is grouped based on rules that associate a defined forwarding class with selected applications for logical system. The match criteria for the rule includes one or more applications. When traffic from a matching application encounters the rule, the rule action sets the forwarding class, and remarks the DSCP value and loss priority to values appropriate for the application.

The AppQoS DSCP rewriter conveys a packet's quality of service through both the forwarding class and a loss priority. The AppQoS rate-limiting parameters control the transmission speed and volume for its associated queues for logical system. The default AppQoS rule set is leveraged from one of the existing AppQoS rule sets, which are configured under the `[edit class-of-service application-traffic-control]` hierarchy level.

Rate limiters are applied in rules based on the application of the traffic for logical system. Two rate limiters are applied for each session: `client-to-server` and `server-to-client`. This usage allows traffic in each direction to be provisioned separately.

Example: Configure Application Quality of Service for Logical Systems

IN THIS SECTION

This example shows how to enable application quality of service (AppQoS) within a logical system to provide prioritization and rate limiting for the traffic.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall configured with logical systems.
- Junos OS Release 19.3R1 and later releases.

Before you begin:

- Read the "Application Quality of Service Support for Logical Systems Overview" on page 398 to understand how and where this procedure fits in the overall support for AppQos.

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

Overview

In this example, you configure an AppQoS rule set and invoke AppQoS as an application service in the logical system. You configure the class of service (CoS) for logical system. The AppQoS rule sets are included in the logical system to implement application-aware quality-of-service control.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems LSYS1 class-of-service application-traffic-control rate-limiters HTTP-BW-RL
bandwidth-limit 512
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
match application junos:HTTP
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
then forwarding-class best-effort
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
then dscp-code-point 001000
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
then loss-priority high
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
then log
set logical-systems LSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1
```

```
then rate-limit server-to-client HTTP-BW-RL
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy from_internet
match source-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy from_internet
match destination-address any
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy from_internet
match application any
set logical-systems LSYS1 security policies from-zone trust to-zone trust policy p1 match
dynamic-application junos:web
set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy from_internet
then permit application-services application-traffic-control rule-set RS1
```

Configuring AppQoS with a 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.

To configure AppQoS with a Logical System:

1. Configure the AppQoS real-time run information about application rate limiting of current or recent sessions for logical system LSYS1.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rate-
limiters HTTP-BW-RL bandwidth-limit 512
```

2. Configure the AppQoS rules and application match criteria for logical system LSYS1.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 match application junos:HTTP
```

3. Configure the AppQoS rules and the forwarding class for logical system LSYS1.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 then forwarding-class best-effort
```

4. Configure the AppQoS rules and the dscp-code-point for logical system LSYS1.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 then dscp-code-point 001000
```

5. Configure the AppQoS rules and the loss priority for logical system LSYS1.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 then loss-priority high
```

6. Assign the rate limiters for rule-sets.

```
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 then log
user@host# set logical-systems LSYS1 class-of-service application-traffic-control rule-sets
RS1 rule RL1 then rate-limit server-to-client HTTP-BW-RL
```

7. Assign the class-of-service rule set to the security policy for logical system LSYS1.

```
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
from_internet match source-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
from_internet match destination-address any
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
from_internet match application any
user@host# set logical-systems LSYS1 security policies from-zone trust to-zone trust policy
p1 match dynamic-application junos:web
user@host# set logical-systems LSYS1 security policies from-zone untrust to-zone trust policy
from_internet then permit application-services application-traffic-control rule-set RS1
```

Results

From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1` 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 LSYS1
security {
```

```
    policies {
        from-zone untrust to-zone trust {
            policy from_internet {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            application-traffic-control {
                                rule-set RS1;
                            }
                        }
                    }
                }
            }
        }
        from-zone trust to-zone trust {
            policy p1 {
                match {
                    dynamic-application junos:web;
                }
            }
        }
    }
}
class-of-service {
    application-traffic-control {
        rate-limiters HTTP-BW-RL {
            bandwidth-limit 512;
        }
        rule-sets RS1 {
            rule RL1 {
                match {
                    application junos:HTTP;
                }
                then {
                    forwarding-class best-effort;
                    dscp-code-point 001000;
                    loss-priority high;
                    rate-limit {
```

```
                    server-to-client HTTP-BW-RL;
                }
                log;
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the class-of-service application-traffic-control counter

Purpose

Verify the class-of-service application-traffic-control counter for logical systems.

Action

To verify the configuration is working properly, enter the `show class-of-service application-traffic-control counter logical-system LSYS1` command.

```
user@host>show class-of-service application-traffic-control counter logical-system LSYS1
Logical System: LSYS1

pic: 0/0
  Counter type                                                Value
 Sessions processed                                           1
 Sessions marked                                              0
```

```
Sessions honored                                    0
Sessions rate limited                               0
Client-to-server flows rate limited                 0
Server-to-client flows rate limited                 0
Session default ruleset hit                         0
Session ignored no default ruleset                  0
```

Meaning

The output displays AppQoS DSCP marking and honoring statistics based on Layer 7 application classifiers.

Verifying the class-of-service application-traffic-control statistics rate-limiter

Purpose

Verify the class-of-service application-traffic-control statistics rate-limiter for logical systems.

Action

To verify the configuration is working properly, enter the `show class-of-service application-traffic-control statistics rate-limiter logical-system LSYS1` command.

```
user@host>show class-of-service application-traffic-control statistics rate-limiter logical-system LSYS1
Logical System: LSYS1

pic: 0/0
```

Meaning

The output displays AppQoS real-time run information about application rate limiting of current or recent sessions.

Logical Systems in a Chassis Cluster

IN THIS SECTION

A chassis cluster provides high availability on SRX Series Firewalls where two devices operate as a single device. Chassis cluster includes the synchronization of configuration files and the dynamic runtime session states between the SRX Series Firewalls, which are part of chassis cluster setup. For more information, see the following topics:

Understanding Logical Systems in the Context of Chassis Cluster

The behavior of a *chassis cluster* whose nodes consist of SRX Series Firewalls 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 primary 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 Firewalls 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.

Starting with Junos OS Release 12.3X48-D50, when you configure the logical systems within a chassis cluster, if logical systems licenses on backup node are not sufficient when you `commit` the configuration, a warning message is displayed about the number of licenses required on backup node as well, just as on primary node in all the previous releases.

SEE ALSO

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Primary Administrators Only) | 407

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) (Primary Administrators Only) | 451

Understanding the Interconnect Logical System and Logical Tunnel Interfaces | 9

Understanding Logical Systems for SRX Series Firewalls | 5

Chassis Cluster Overview

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Primary Administrators Only)

IN THIS SECTION

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

NOTE: The primary administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the primary 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 SRX Series Firewalls with identical hardware configurations. See *Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices*. This chassis cluster deployment scenario includes the configuration of the SRX Series Firewall 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 or SRX1500 devices or the SRX3000 line, you can configure the fabric ports only. (Platform support depends on the Junos OS release in your installation.) See *Connecting SRX Series Devices to Create a Chassis Cluster*.
- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See *Example: Setting the Node ID and Cluster ID for Security Devices in a Chassis Cluster* .

NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the primary administrator. Log in to the device as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

NOTE: When you use SRX Series Firewalls 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.

Overview

IN THIS SECTION

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

- Primary logical system—The primary administrator configures a security profile to provision portions of the system's security resources to the primary logical system and configures the resources of the primary logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The primary 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 primary administrator configures logical tunnel interfaces between the interconnect logical system and each logical system. These peer interfaces effectively allow for the establishment of tunnels.

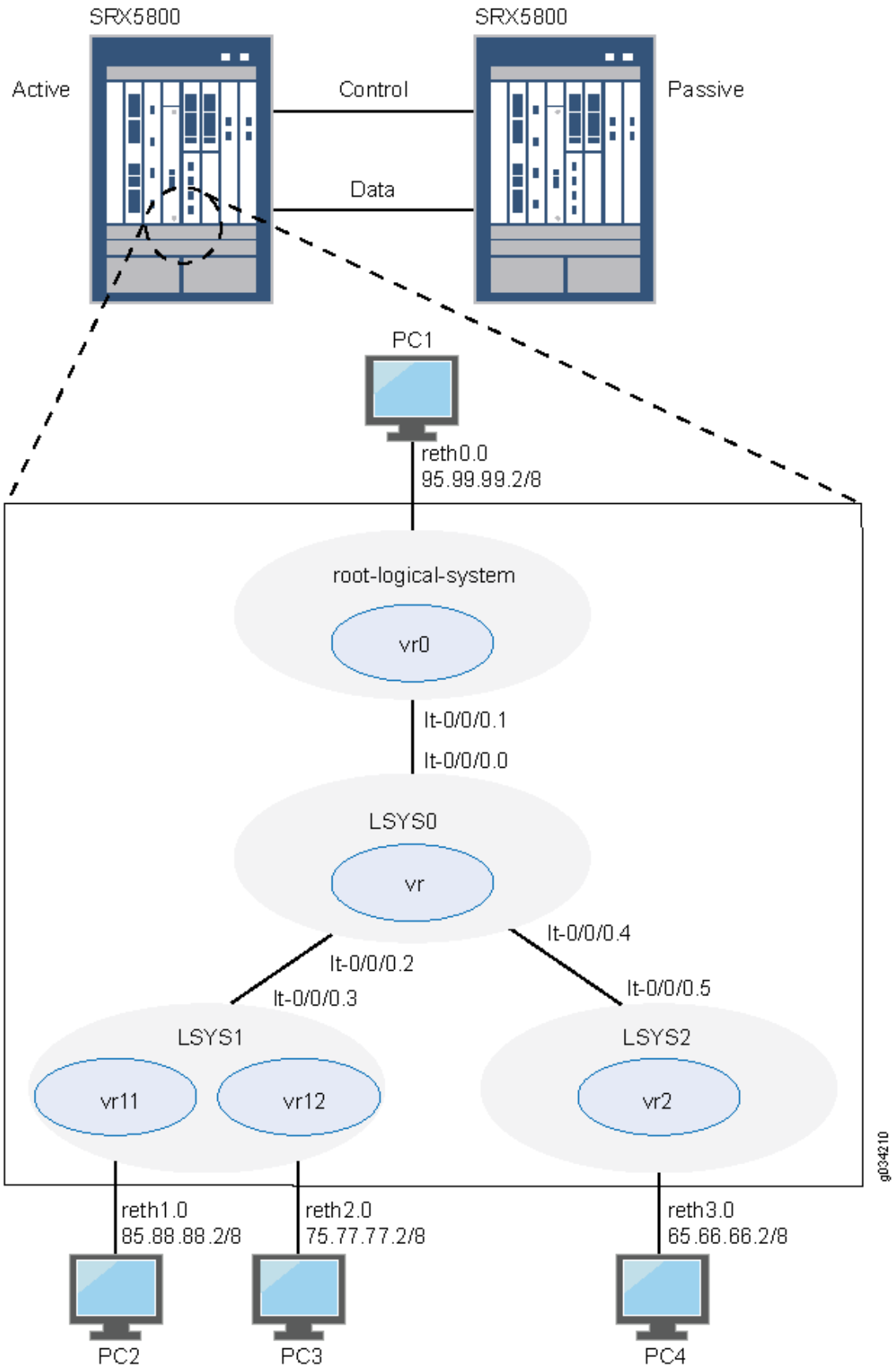
NOTE: This example does not describe configuring features such as NAT, IDP, or VPNs for a logical system. See "SRX Series Logical Systems Primary Administrator Configuration Tasks Overview" on page 22 and "User Logical Systems Configuration Overview" on page 48 for more information about features that 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 for NAT (CLI Procedure)*.

Topology

Figure 10 on page 410 shows the topology used in this example.

Figure 10: Logical Systems in a Chassis Cluster



Configuration

IN THIS SECTION

Chassis Cluster Configuration (Primary Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the primary 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 (Primary Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the primary 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*.

To create logical systems and user logical system administrators and configure the primary 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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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 primary logical system.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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 primary 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 in to his or her user logical system. The primary 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*.

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

IN THIS SECTION

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

Identify any chassis cluster issues by looking at the 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
```

SEE ALSO

Understanding Logical Systems in the Context of Chassis Cluster | **406**

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (IPv6) (Primary Administrators Only) | **451**

Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices

Chassis Cluster Overview

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

IN THIS SECTION

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

NOTE: The primary administrator configures the chassis cluster and creates logical systems (including an optional interconnect logical system), administrators, and security profiles. Either the primary 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 SRX Series Firewalls with identical hardware configurations. See *Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices*. This chassis cluster deployment scenario includes the configuration of the SRX Series Firewall 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 or SRX1500 devices or the SRX3000 line, you can configure the fabric ports only. (Platform support depends on the Junos OS release in your installation.)
- Set the chassis cluster ID and node ID on each device and reboot the devices to enable clustering. See *Example: Setting the Node ID and Cluster ID for Security Devices in a Chassis Cluster* .

NOTE: For this example, chassis cluster and logical system configuration is performed on the primary (node 0) device at the root level by the primary administrator. Log in to the device as the primary administrator. See "Understanding the Primary Logical Systems and the Primary Administrator Role" on page 21.

NOTE: When you use SRX Series Firewalls 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.

Overview

IN THIS SECTION

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

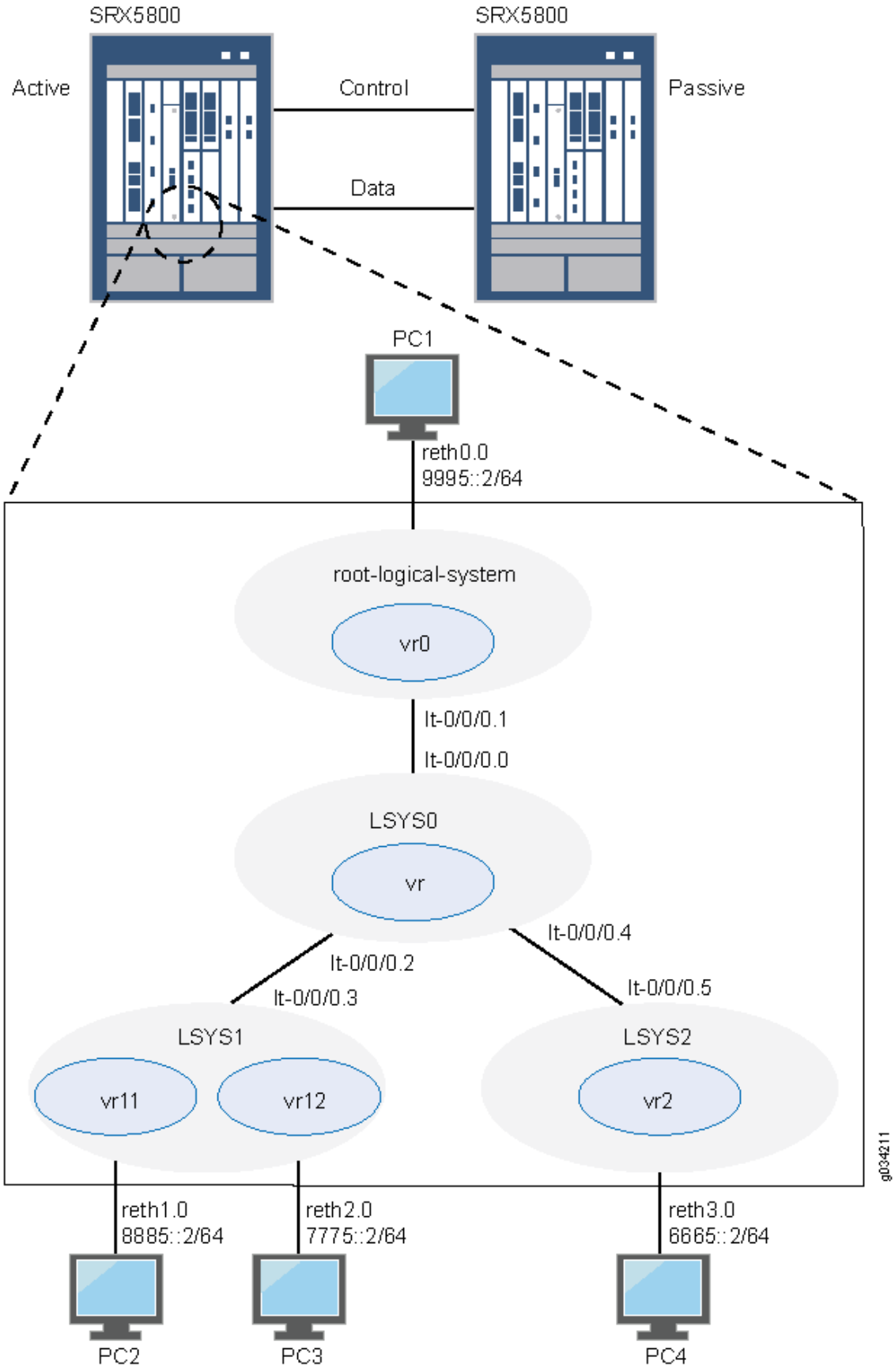
- Primary logical system—The primary administrator configures a security profile to provision portions of the system's security resources to the primary logical system and configures the resources of the primary logical system.
- User logical systems LSYS1 and LSYS2 and their administrators—The primary 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 primary 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 Systems Primary Administrator Configuration Tasks Overview" on page 22 and "User Logical Systems Configuration Overview" on page 48 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 for NAT (CLI Procedure)*.

Topology

Figure 11 on page 454 shows the topology used in this example.

Figure 11: Logical Systems in a Chassis Cluster (IPv6)



Configuration

IN THIS SECTION

Chassis Cluster Configuration with IPv6 Addresses (Primary Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the primary 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 (Primary Administrator)

CLI Quick Configuration

To quickly create logical systems and user logical system administrators and configure the primary 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*.

To create logical systems and user logical system administrators and configure the primary 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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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 primary logical system.

   Step-by-Step Procedure

   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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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 primary 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 in to his or her user logical system. The primary 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*.

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

IN THIS SECTION

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
```

SEE ALSO

Understanding Logical Systems in the Context of Chassis Cluster | 406

Example: Configuring Logical Systems in an Active/Passive Chassis Cluster (Primary Administrators Only) | 407

Example: Configuring an Active/Passive Chassis Cluster on SRX5800 Devices

Chassis Cluster Overview

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
12.3X48-D50	Starting with Junos OS Release 12.3X48-D50, when you configure the logical systems within a chassis cluster, if logical systems licenses on backup node are not sufficient when you `commit` the configuration, a warning message is displayed about the number of licenses required on backup node as well, just as on primary node in all the previous releases.

Flow Trace for Logical Systems

IN THIS SECTION

Flow trace also called traceoptions, allows you to monitor traffic flow into and out of an SRX Series Firewall. You can use tracoptions as debugging tool to trace the packets as they traverse the SRX Series Firewall. Traceoptions help you to get details of actions by your security device.

Flow Trace Support for Logical Systems Overview

For an SRX Series Firewall configured with logical systems, by default the traceoptions are configured at the root level only. In this case, all the system traces including root and logical systems are logged in one single trace file. This generated large amounts of information in a single file.

Starting in Junos OS Release 19.4R1, you can enable tracing operations per logical system level. When you configure the traceoptions at the logical system level, then the traces for that specific logical systems are logged in the respective trace file. You can generate an output file for the specified logical system, and you can find the required traffic information easily in the trace file.

When you enable traceoptions, you specify the name of the file and the type of information you want to trace.

All flow trace sent to one log file in root, if you enable the traceoptions under root context. Traces for a logical system only sent to the respective trace file, if you enable the traceoptions for the specific logical system.

Configure Flow Trace Support for Logical Systems

Configuring traceoptions for a logical system includes configuring both a target file and a flag. The target file determines where the trace output is recorded. The flag defines what type of data to be collected. If you configure traceoptions for a logical system, the respective trace file sent to the specific logical system log file only.

To configure traceoptions for a logical system:

1. Create logical system `LSYS1` and setup the basic configurations. See "Setting Up a Logical System" on page 52
2. Configure target file to save the trace information for the logical system.

```
[edit]
user@host# set logical-systems LSYS1 security flow traceoptions file flow_lsys1.log
user@host# set logical-systems LSYS1 security flow traceoptions file size 1g
```

3. Configure traceoptions flag for the logical system.

```
[edit]
user@host# set logical-systems LSYS1 security flow traceoptions flag all
```

After you commit the traceoptions configuration, you can view the traceoptions debug files for the logical system using `show log` *`tracefilename`* operational command.

```
user@host:LSYS1> show log flow_lsys1.log
Nov  7 07:34:09 07:34:09.491800:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock

Nov  7 07:34:09 07:34:09.491809:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491840:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock
```

```
Nov  7 07:34:09 07:34:09.491841:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491854:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh 0x0

Nov  7 07:34:09 07:34:09.491868:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock

Nov  7 07:34:09 07:34:09.491869:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491881:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh 0x0
```

Example: Deleting a Logical System

IN THIS SECTION

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

IN THIS SECTION

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.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
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.

Step-by-Step Procedure

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
```

3. Delete the login classes.

Step-by-Step Procedure

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 "$ABC123"; ## 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 "$ABC123"; ## 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
```

4. 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

IN THIS SECTION

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

Purpose

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

RELATED DOCUMENTATION

Understanding User Logical Systems and the User Logical System Administrator Role | 50

Understanding Logical Systems for SRX Series Firewalls | 5

Troubleshooting Logical Systems

IN THIS SECTION

Use the following features to monitor logical systems and troubleshoot the software issues. For more information, see the following topics:

Understanding Security Logs and Logical Systems

IN THIS SECTION

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. The logical system log 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 primary administrator can configure logging at the [`edit security log`] hierarchy level. User logical system administrators cannot configure logging for their logical systems.

Stream mode is a set of logging services that includes:

- Off-box logging (SRX Series)
- On-box logging and reporting (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, SRX4100, SRX4200, and SRX4600 Series)

Per logical system configuration is supported for the off-box logging and logs are handled based on these configurations. Previously the user logical system logs were generated from root logical system. For off-box logging, the logical system logs can only be generated from logical system interface.

Limitations

Each SPU can only support a maximum of 1000 connections for standalone and 500 connections for cluster on the SRX5400, SRX5600, and SRX5800 devices in the Junos OS 18.2R1 release. If all the connections are used up, some connections for user logical systems might not be established.

NOTE: The error message will be captured in the System Log Explorer.

Configuring On-Box Reporting for logical Systems

SRX Series Firewalls supports different types of reports for logical system users.

Reports are stored locally on the SRX Series Firewall and there is no requirement for separate devices or tools for logs and reports storage. The on-box reports provides a simple and easy-to-use interface for viewing the security logs.

Before you begin:

- Understand how to configure security log for logical systems. See Example: Configure Security Log for logical Systems

To configure on-box reporting for logical system:

1. Define the logical system name as LSYS1.

```
user@host# set logical-systems LSYS1
```

2. Create report within security log per tenant system.

```
user@host# set logical-systems LSYS1 security log report
```

3. Confirm your configuration by entering the `show logical-systems LSYS1` command.

```
user@host# show logical-systems LSYS1
security {
    log {
        report;
    }
}
```

NOTE: By default the `report` option is disabled. The `set logical-systems LSYS1 security log mode stream` command is enabled by default.

Example: Configure Security Log for Logical Systems

IN THIS SECTION

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

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand how to configure a logical system.
- Understand how to create security profiles for the primary logical system. See Understanding Logical Systems Security Profiles (Primary Administrators Only).

Overview

SRX Series Firewalls have two types of log: system logs and security logs. System logs record control plane events, for example, admin login to the device. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy.

The two types of logs can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

For off-box logging, security logs for a logical system are sent from a logical system interface. If the logical system interface is already configured in a routing instance, then configure `routing-instance routing-instance-name` at `edit logical-systems logical-system-name security log stream log-stream-name host` hierarchy. If the interface is not configured in routing instance, then no routing instance should be configured at `edit logical-systems logical-system-name security log stream log-stream-name host` hierarchy.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set logical-systems LSYS1 security log mode stream
set logical-systems LSYS1 security log stream LSYS1_s format binary host 1.3.54.22
set logical-systems LSYS1 security log source-address 2.3.45.66
set logical-systems LSYS1 security log transport protocol tls
set logical-systems LSYS1 routing-instances LSYS1_ri instance-type virtual-router
set logical-systems LSYS1 routing-instances LSYS_ri interface ge-0/0/3
set logical-systems LSYS1 security log stream LSYS1_s host routing-instance LSYS1_ri
set system security-profile p1 security-log-stream-number reserved 1
set system security-profile p1 security-log-stream-number maximum 2
set system security-profile LSYS1_profile logical-system LSYS1
```

Procedure

Step-by-Step Procedure

The following procedure specifies how to configure security logs for a logical system.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging.

```
[edit ]
user@host# set logical-systems LSYS1 security log mode stream
user@host# set logical-systems LSYS1 security log stream LSYS1_s format binary host 1.3.54.22
```

2. For off-box security logging, specify the source address, which identifies the SRX Series Firewall that generated the log messages. The source address is required.

```
[edit ]
user@host# set logical-systems LSYS1 security log source-address 2.3.45.66
```

3. Specify the routing instance and define the interface.

```
[edit ]
user@host# set logical-systems LSYS1 routing-instances LSYS1_ri instance-type virtual-router
user@host# set logical-systems LSYS1 routing-instances LSYS_ri interface ge-0/0/3
```

4. Define routing instance for a logical system.

```
[edit ]
user@host# set logical-systems LSYS1 security log stream LSYS1_s host routing-instance
LSYS1_ri
```

5. Specify the security log transport protocol for the device.

```
[edit ]
user@host# set logical-systems LSYS1 security log transport protocol tls
```

Procedure

Step-by-Step Procedure

The following procedure specifies how to configure a security profile for a logical system.

1. Configure a security profile and specify the number of maximum and reserved policies.

```
[edit ]
user@host# set system security-profile p1 security-log-stream-number reserved 1
user@host# set system security-profile p1 security-log-stream-number maximum 2
```

2. Assign the configured security profile to TSYS1.

```
[edit ]
user@host# set system security-profile LSYS1_profile logical-system LSYS1
```

Results

From configuration mode, confirm your configuration by entering the `show system security-profile`, `show logical-systems LSYS1 security log`, and `show logical-systems LSYS1 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 system security-profile
LSYS1_profile {
    logical-system LSYS1;
}
p1 {
    security-log-stream-number {
        maximum 2;
        reserved 1;
    }
}
```

```
[edit]
user@host# show logical-systems LSYS1 security log
mode stream;
source-address 2.3.45.66;
transport {
    protocol tls;
}
stream LSYS1_s {
```

```
    format binary;
    host {
        1.3.54.22;
    }
}
```

```
[edit]
user@host# show logical-systems LSYS1 routing-instances
LSYS1_ri {
    instance-type virtual-router;
    interface ge-0/0/3.0;
}
```

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

Verification

IN THIS SECTION

- Verifying Detailed Output for Security Log | **511**

Verifying Detailed Output for Security Log

Purpose

Verify that the output displays the resource information for all logical systems.

Action

From operational mode, enter the `show system security-profile security-log-stream-number tenant all` command.

```
logical-system name  security profile name  usage    reserved    maximum

root-logical-system         Default-Profile           0          0
```

Meaning

The output displays the resource information for logical systems.

Configuring On-Box Binary Security Log Files for Logical System

SRX Series devices support two types of log: system logs and security logs.

The two types of log are collected and saved either on-box or off-box. The following procedure explains how to configure security logs in binary format for on-box (event-mode) logging for logical system.

The following procedure specifies binary format for event-mode security logging, and defines the log filename, path, and log file characteristics for logical system.

1. Specify the logging mode and the format for the log file. For on-box, event-mode logging:

```
[edit]
user@host# set logical-systems LSYS1 security log mode event
user@host# set logical-systems LSYS1 security log format binary
```

2. (Optional) Specify a log filename.

```
[edit]
user@host# set logical-systems LSYS1 security log file name security-binary-log
```

NOTE: Security log filename is not mandatory. If security log filename is not configured, by default the file bin_messages is created in the /var/log directory.

3. Confirm your configuration by entering the `show logical-systems LSYS1` command.

```
[edit]
user@host# show logical-systems LSYS1
security {
    log {
        mode event;
        format binary;
        file {
            name security-binary-log;
```

```
        }
    }
}
```

The following procedure specifies binary format for stream-mode security logging, and defines the log filename and log file characteristics for logical system.

1. Specify the logging mode and the format for the log file. For on-box, stream-mode logging:

```
[edit]
user@host# set logical-systems LSYS1 security log mode stream
user@host# set logical-systems LSYS1 security log stream s1 format binary
```

2. (Optional) Specify a log filename.

```
[edit]
user@host# set logical-systems LSYS1 security log stream s1 file name f1.bin
```

3. Confirm your configuration by entering the `show logical-systems LSYS1` command.

```
[edit]
user@host# show logical-systems LSYS1
security {
    log {
        mode stream;
        stream s1 {
            format binary;
            file {
                name f1.bin;
            }
        }
    }
}
```

Configuring Off-Box Binary Security Log Files for Logical System

SRX Series devices support two types of log: system logs and security logs.

The two types of log can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

The following procedure specifies binary format for stream-mode security logging, and defines the logging mode, source address, and host name characteristics for logical system.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging:

```
[edit]
user@host# set logical-systems LSYS1 security log mode stream s1 format binary
```

2. Specify the source address for off-box security logging.

```
[edit]
user@host# set logical-systems LSYS1 security log source-address 100.0.0.1
```

3. Specify the host name.

```
[edit]
user@host# set logical-systems LSYS1 security log stream s1 host 100.0.0.2
```

4. Confirm your configuration by entering the `show logical-systems LSYS1` command.

```
[edit]
user@host#show logical-systems LSYS1
security {
    log {
        mode stream;
        source-address 100.0.0.1;
        stream s1 {
            format binary;
            host {
                100.0.0.2;
            }
        }
    }
}
```

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 primary 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 primary administrator configures end-to-end event tracing, the trace output contains logical system information.

The primary 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.

Data path debugging is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800.

SEE ALSO

Performing Tracing for Logical Systems (Primary Administrators Only) | 515

Performing Tracing for Logical Systems (Primary Administrators Only)

> **NOTE**: Only the primary 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 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 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
```

SEE ALSO

Understanding Data Path Debugging for Logical Systems | 515

Troubleshooting DNS Name Resolution in Logical System Security Policies (Primary Administrators Only)

IN THIS SECTION

Problem

Description

The address of a hostname in an address book entry that is used in a security policy might fail to resolve correctly.

Cause

Normally, address book entries that contain dynamic hostnames refresh automatically for SRX Series Firewalls. The TTL field associated with a DNS entry indicates the time after which the entry should be refreshed in the policy cache. Once the TTL value expires, the SRX Series Firewall automatically refreshes the DNS entry for an address book entry.

However, if the SRX Series Firewall is unable to obtain a response from the DNS server (for example, the DNS request or response packet is lost in the network or the DNS server cannot send a response), the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found.

Solution

The primary administrator can use the `show security dns-cache` command to display DNS cache information on the SRX Series Firewall. If the DNS cache information needs to be refreshed, the primary administrator can use the `clear security dns-cache` command.

NOTE: These commands are only available to the primary administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

SEE ALSO

- Understanding Logical Systems Security Policies

RELATED DOCUMENTATION

- Security Profiles for Logical Systems | **67**

3

CHAPTER

Tenant Systems

Tenant Systems Overview

IN THIS SECTION

A tenant system supports routing, services and security features.

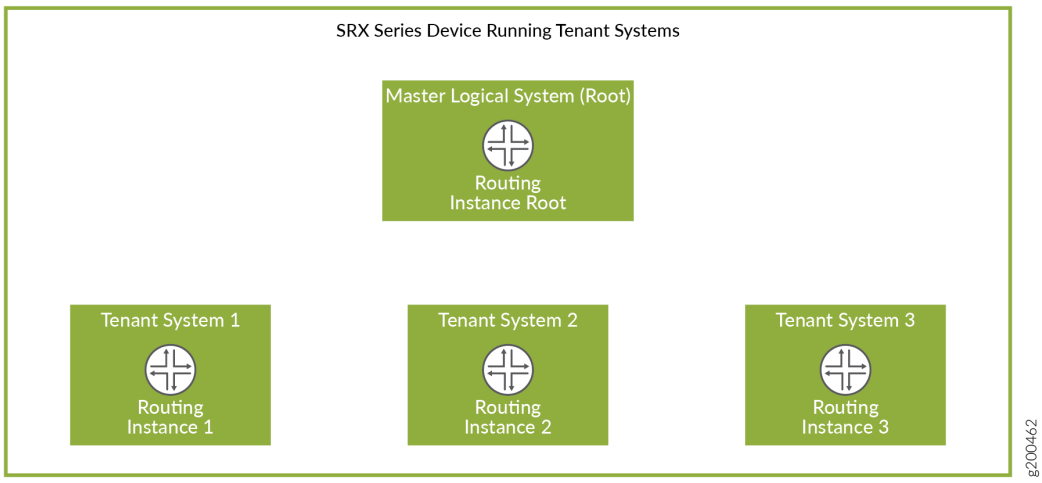
Understanding Tenant Systems

IN THIS SECTION

A tenant system logically partitions the physical firewall into separate and isolated logical firewall. Although similar to logical systems, tenant systems have much higher scalability and fewer routing features. Each tenant system on a device allows you to control a discrete administrative domain for security services. By transforming your device into a multitenant system, you can provide various departments, organizations, customers, and partners—depending on your environment—private and logically separated use of system resources and tenant-specific views of security configuration and KPIs.

A primary administrator creates and manages all the tenant systems. Figure 12 on page 526 shows a single device with a primary logical system and discrete tenant systems.

Figure 12: Tenant Systems



Differences Between Logical Systems and Tenant Systems

Table 27 on page 526 describes the key differences between logical systems and tenant systems.

Table 27: Differences Between Logical Systems and Tenant Systems

Functionality	Logical Systems	Tenant Systems
Feature support	Supports all the routing features to provide optimal data routing paths.	Supports routing features and high-scale security virtualization to isolate customer environments.
Scalability	A maximum of 32 logical systems can be configured on a physical SRX Series Firewall.	A maximum of 500 tenant systems can be configured on a physical SRX Series Firewall to provide high scalability.

Table 27: Differences Between Logical Systems and Tenant Systems *(Continued)*

Functionality	Logical Systems	Tenant Systems
Routing protocol process	Every logical system needs an individual copy of the routing protocol process to logically separate the resources on a device.	The primary logical system has a single routing protocol process, which is shared by the tenant systems. Routing instances supported by this single routing protocol process achieve the security resource separation on the firewall.
Routing instance	A default routing instance is automatically created for every logical system.	Starting in Junos OS Release 19.2R1, the virtual-router configured in a tenant system is passed as the default routing-instance to `ping`, `telnet`, `ssh`, `traceroute`, `show arp`, `clear arp`, `show ipv6 neighbors`, and `clear ipv6 neighbors` commands.
Logical interface configuration	The primary administrator assigns the logical interfaces and the logical system administrator can configure the interface attributes.	A tenant system administrator cannot configure the logical interfaces. The primary administrator assigns the logical interfaces to a tenant system.

Use Cases for Logical Systems and Tenant Systems

A logical system is used when more than one virtual router is required. For example, you have multiple connections to the external network and they cannot co-exist in the same virtual router. Tenant systems are used when you need to separate departments, organization, or customers and each of them can be limited to one virtual router. The main difference between a logical system and a tenant system is that a logical system supports advanced routing functionality using multiple routing instances. In comparison, a tenant system supports only one routing instance, but supports the deployment of significantly more tenants per system.

Deployment Scenarios for Multitenant Systems

You can deploy an SRX Series Firewall running a multitenant system in many environments such as a managed security service provider (MSSP), an enterprise network, or a branch office segment. Table 28 on page 528 describes the various deployment scenarios and the roles played by the tenant systems in such scenarios.

Table 28: Deployment Scenarios with Respect to Tenant Systems

Deployment Scenarios	Roles of a Tenant System
Managed security service provider (MSSP)	• In a managed security service provider (MSSP), each customer can be isolated from other customer to protect data privacy. Customers that require defined service level agreements (SLAs) can be be allocated memory and system resources to meet these SLAs. • The customer can configure distinct security policies for compliance and control per tenant system.
Enterprise network	• A tenant system can be assigned to a workgroup, department, or other organizational construct within an enterprise. • A tenant system can define the distinct security policies for the enterprise workgroup, department, or other organizational construct of the enterprise.
Branch office segment	• In a branch office, a tenant system can individually manage and segregate corporate and guest traffic. • Advanced security policies can be configured per tenant system; this approach allows granular control of the security policies. • A tenant system provides ease of management and troubleshooting.

Benefits of Tenant Systems

- Curtail cost by reducing the number of physical devices required for your organization. You can consolidate services for various groups of users on a single device and reduce the hardware costs, power expenditure, and rack space.
- Provide isolation and logical separation at the tenant system level. Provides the ability to separate tenant systems with administrative separation at large scale in which each tenant system can define its own security controls and restrictions without impacting other tenant systems.

Roles and Responsibilities of Primary Administrator and Tenant System Administrator

A primary administrator creates and manages all the tenant systems. A primary logical system is created at the root level and is allocated a single routing protocol process. Although this routing protocol process is shared, tenant systems enable logical resource separation on the firewall. By default, all system resources are assigned to the primary logical system, and the primary administrator allocates them to the tenant system administrators.

NOTE: In Junos OS command-line reference, primary logical system is referred as root logical system.

A tenant system is created that is subtended by the primary logical system. Although all the tenants under the primary logical system share a single routing process, each tenant system has a single routing instance. Table 29 on page 530 describes the roles and responsibilities of the primary administrator and tenant system administrator.

Table 29: Roles and Responsibilities With Respect to Tenant Systems

Roles	Definition	Responsibilities
Primary administrator	A user account with superuser configuration and verification privileges for all logical systems and tenant systems.	• View and access all logical systems and tenant systems. • Create login accounts for all the tenant systems and assign the login accounts to the appropriate tenant system. • Create and allocate the resources to the tenant systems. • Create one custom routing instance under the tenant system which acts as the default routing instance for the tenant system. • Create a virtual router under the tenant system and assign it to the tenant system. • Create logical interfaces to assign to the tenant systems. • Manage the tenant systems in the primary logical system. • Ensure duplicate names for tenant system, logs, and trace file do not exist.

Table 29: Roles and Responsibilities With Respect to Tenant Systems *(Continued)*

Roles	Definition	Responsibilities
Tenant system administrator	A tenant system account with all configuration and verification privileges. **NOTE**: The configuration and verification privileges of a tenant system administrator depends on the permission assigned to them by the primary administrator while creating the tenant system administrator. Multiple tenant system administrators can be created for a tenant system with different permission levels based on your requirement.	• Access and view the resources of the tenant system. • Configure the resources allocated and routing protocols. • Configure schedulers, security profiles, and security features. The following privileges are not supported by the tenant system administrator: • Define access restrictions and the default routing instance for the tenant system. • Access and view the resources of other tenant systems. • Modify the number of allocated resources for a tenant system. • Create logical interfaces, virtual router, and policy options.

Tenant System Capacity

The maximum number of tenant systems that can be created on the device are listed in Table 30 on page 531.

Table 30: Tenant Systems Capacity

Platform	Logical Systems Capacity	Tenant Systems Capacity for Junos OS Release 18.4R1	Tenant Systems Capacity starting in Junos OS Release 20.1R1	Tenant Systems Capacity starting in Junos OS Release 23.4R1
SRX1500	32	50	50	
SRX1600	32			50

Table 30: Tenant Systems Capacity *(Continued)*

Platform	Logical Systems Capacity	Tenant Systems Capacity for Junos OS Release 18.4R1	Tenant Systems Capacity starting in Junos OS Release 20.1R1	Tenant Systems Capacity starting in Junos OS Release 23.4R1
SRX2300	32			200
SRX4100 and SRX4200	32	200	200	
SRX4600	32	300	300	
SRX5400, SRX5600, and SRX5800 Series devices with SPC2 cards	32	100	100	
SRX5400, SRX5600, and SRX5800 Series devices with SPC3 cards	32	500	500	
SRX5400, SRX5600, and SRX5800 Series devices with SPC2 and SPC3 cards	32	100	100	
vSRX	8		42	

NOTE: Starting in Junos OS Release 20.1R1, vSRX Virtual Firewall and vSRX3.0 instances with a memory capacity of 16GB or more and at least two CPUs in the Routing Engine support logical systems and tenant systems.

Starting in Junos OS Release 18.4R1, tenant systems can be supported on an SRX5000 line security services gateway equipped with a combination of third generation service processing cards (SRX5K-SPC3) and second generation service processing cards (SRX5K-SPC-4-15-320). Prior to Junos OS Release 18.4R1, tenant systems was supported on SPC2 only.

SEE ALSO

Primary Logical Systems Overview | 20

Tenant System Configuration Overview

The primary administrator creates a tenant system and assigns an administrator for managing the tenant system. A tenant system can have multiple administrators. The roles and responsibilities of a tenant system administrator are explained in "Understanding Tenant Systems" on page 525.

The primary administrator configures the logical interfaces and assigns those interfaces to the tenant system. Configure one routing instance and the routing protocols, and add options for the routing instance. See "Configuring a Routing Instance for a Tenant System" on page 535.

Tenant systems have their own configuration database. After successful configuration, the changes are merged to the primary database for each tenant systems. Multiple tenant systems can perform configuration changes at a time. You can commit the changes for only one tenant at a time. If the primary administrator and a tenant system administrator performs configuration changes simultaneously, the configuration changes performed by the primary administrator override the configuration changes performed by the tenant system administrator.

The following steps explain the tasks that the tenant system administrator performs to configure the security features in a tenant system:

1. Use the SSH service to access the device, and then log in to the tenant system with the login ID and password provided by the primary administrator.

   ```
   login: <tenant_name>
   password: <password>
   ```

   After you are authenticated, the presence of the “>” prompt indicates that you accessed to the CLI operational mode. The prompt is preceded by a string that contains the username, the hostname of the device, and the name of the tenant system. When the CLI starts, you are at the top level in operational mode.

   ```
   TSYS1_admin1@host:TSYS1>
   ```

2. Access the configuration mode by entering the `configure` command.

```
TSYS1_admin1@host:TSYS1> configure
TSYS1_admin1@host:TSYS1#
```

3. Enter the **quit** command to exit the configuration mode and return to the CLI operational mode.

```
TSYS1_admin1@host:TSYS1# quit
TSYS1_admin1@host:TSYS1>
```

4. Configure the following security features in the tenant system as necessary:

   - Create zones for the tenant system and bind the logical interfaces to the zones. Create address books and use them in the security policies. See "Example: Configuring Zones in the Tenant System" on page 570.

   - Configure screen options at the zone level. See Example: Configuring Screen Options for a Tenant System.

   - Configure security policies between zones in the tenant system. See Example: Configuring Security Policies in a Tenant System.

     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.

   - Configure firewall authentication to the tenant system. The primary administrator creates access profiles in the primary logical system. The tenant 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 "Configuring Firewall Authentication for a Tenant System" on page 616.

   - Configure Network Address Translation (NAT) for the tenant system. See Example: Configuring Network Address Translation for the Tenant Systems.

   - Configure Application Layer Gateway (ALG) for the tenant system. See Example: Configuring ALG in Tenant System.

   - Configure Intrusion Detection and Prevention (IDP) policies and attacks for the tenant system. See "Example: Configuring IDP Policies and Attacks for Tenant Systems" on page 690.

Configuring a Routing Instance for a Tenant System

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. A set of interfaces that belong to the routing instance and the routing protocol parameters control the information in the routing instance. A tenant system can configure the assigned routing instance and the interfaces that belong to the routing instance within a tenant system.

NOTE: Only one routing instance can be created for a tenant system.

The following procedure describes the steps to configure a routing instance and interfaces in a routing table for a tenant system:

1. Create a tenant system named `TSYS1`.

```
[edit]
user@host# set tenants TSYS1
```

2. Create a routing instance `r1` and assign the routing instance type for the tenant system.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 instance-type virtual-router
```

3. Specify the interface name for the routing instance.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 interface lt-0/0/0.101
user@host# set tenants TSYS1 routing-instances r1 interface xe-0/0/0.0
user@host# set tenants TSYS1 routing-instances r1 interface xe-0/0/1.0
```

4. Specify the routing option for the routing instance.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 routing-options router-id 1.1.1.101
```

5. Commit the configuration.

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

To view the configuration for the tenant system TSYS1, run the show tenants TSYS1 command.

```
routing-instances {
    r1 {
        instance-type virtual-router;
        interface lt-0/0/0.101;
        interface xe-0/0/0.0;
        interface xe-0/0/1.0;
        routing-options {
            router-id 1.1.1.101;
        }
    }
}
```

The show tenants TSYS1 command displays all the routing instance parameters configured for the tenant system TSYS1.

Understanding Routing and Interfaces for Tenant Systems

IN THIS SECTION

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The interfaces are used for forwarding data for the routing instance, and to learn the routing information from other peers (SRX Series Firewalls) using routing protocols.

A Logical interface (IFL) can be defined at either one of the following levels:

- Global level (root logical system)
- User logical system level
- Tenant system level (Starting from Release Junos OS 18.4R1)

The IFL defined at the global level can be used either in root logical system or in one of the tenant systems. The IFL defined in a tenant system can be used in that tenant system only.

Default routing instance is not available for tenant systems. So, when a custom routing instance is created for a tenant system, all the interfaces defined in that tenant system should be added to that routing instance.

Overview: Configuring Routing and Interfaces for Tenant Systems

IN THIS SECTION

This overview shows how to configure interfaces and routing instances for a tenant system.

Requirements

Before you begin:

- Determine which logical interfaces and, optionally, which logical tunnel interfaces are allocated. See Tenant System Configuration Overview.

Overview

The following procedure describes the steps to configure a routing instance and interfaces in a routing table within a tenant system.

This topic configures the interfaces and routing instances described in Table 31 on page 537.

Table 31: User Tenant System Interface and Routing Instance Configuration

Feature	Name	Configuration Parameters
Interface	ge-0/0/2.1 ge-0/0/2.2 ge-0/0/2.3	• IP address 10.0.0.1/24 • IP address 10.0.0.2/24 • IP address 10.0.0.3/24

Table 31: User Tenant System Interface and Routing Instance Configuration *(Continued)*

Feature	Name	Configuration Parameters
Routing instance	r1 r2	• Instance type: virtual router • Includes interfaces ge-0/0/2.1, ge-0/0/2.3, and ge-0/0/2.2

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2.3 vlan-id 103
set interfaces ge-0/0/2.3 family inet address 10.0.0.3/24
set tenants TSYS1
set tenants TSYS1 interfaces ge-0/0/2.1 vlan-id 101
set tenants TSYS1 interfaces ge-0/0/2.1 family inet address 10.0.0.1/24
set tenants TSYS1 routing-instances r1 instance-type virtual-router
set tenants TSYS1 routing-instances r1 interface ge-0/0/2.1
set tenants TSYS1 routing-instances r1 interface ge-0/0/2.3
set tenants TSYS2
set tenants TSYS2 interfaces ge-0/0/2.2 vlan-id 102
set tenants TSYS2 interfaces ge-0/0/2.2 family inet address 10.0.0.2/24
```

```
set tenants TSYS2 routing-instances r2 instance-type virtual-router
set tenants TSYS2 routing-instances r2 interface ge-0/0/2.2
```

Step-by-Step Procedure

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

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

1. Configure the interfaces to support VLAN tagging.

```
[edit]
user@host# set interfaces ge-0/0/2 vlan-tagging
```

2. Configure the IFL at the root level.

```
[edit]
set interfaces ge-0/0/2.3 vlan-id 103
set interfaces ge-0/0/2.3 family inet address 10.0.0.3/24
```

3. Create a tenant system named TSYS1.

```
[edit]
user@host# set tenants TSYS1
```

4. Define the Interface in the tenant system TSYS1.

```
[edit]
user@host# set tenants TSYS1 interfaces ge-0/0/2.1 vlan-id 101
user@host# set tenants TSYS1 interfaces ge-0/0/2.1 family inet address 10.0.0.1/24
user@host# set tenants TSYS1 routing-instances r1 interface ge-0/0/2.3
```

5. Create a routing instance r1 and assign the routing instance type for the tenant system.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 instance-type virtual-router
```

6. Specify the interface name for the routing instance.

```
[edit]
user@host# set tenants TSYS1 routing-instances r1 interface ge-0/0/2.1
```

7. Create a tenant system named TSYS2.

```
[edit]
user@host# set tenants TSYS2
```

8. Define the Interface in the tenant system TSYS2.

```
[edit]
user@host# set tenants TSYS2 interfaces ge-0/0/2.2 vlan-id 102
user@host# set tenants TSYS2 interfaces ge-0/0/2.2 family inet address 10.0.0.2/24
```

9. Create a routing instance r2 and assign the routing instance type for the tenant system.

```
[edit]
user@host# set tenants TSYS2 routing-instances r2 instance-type virtual-router
```

10. Specify the interface name for the routing instance.

```
[edit]
user@host# set tenants TSYS2 routing-instances r2 interface ge-0/0/2.2
```

11. Commit the configuration.

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

Results

From configuration mode, confirm your configuration by entering the `show interfaces` and `show tenants` 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-0/0/2 {
    vlan-tagging;
    unit 3 {
        vlan-id 103;
        family inet {
            address 10.0.0.3/24;
        }
    }
}
```

```
[edit]
user@host# show tenants
TSYS1 {
    interfaces {
        ge-0/0/2 {
            unit 1 {
                vlan-id 101;
                family inet {
                    address 10.0.0.1/24;
                }
            }
        }
    }
    routing-instances {
        r1 {
            instance-type virtual-router;
            interface ge-0/0/2.1;
            interface ge-0/0/2.3;
        }
    }
}
TSYS2 {
    interfaces {
```

```
        ge-0/0/2 {
            unit 2 {
                vlan-id 102;
                family inet {
                    address 10.0.0.2/24;
                }
            }
        }
    }
    routing-instances {
        r2 {
            instance-type virtual-router;
            interface ge-0/0/2.2;
        }
    }
}
```

The `show tenants` command displays all the interfaces that are defined in the tenant systems `TSYS1` and `TSYS2`, and the routing instance parameters configured for both the tenant systems.

```
user@host> show interfaces ge-0/0/2.1 detail
  Logical interface ge-0/0/2.1 (Index 89) (SNMP ifIndex 548) (Generation 161)
    Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.101 ]  Encapsulation: ENET2
    Tenant Name: TSYS1
    Traffic statistics:
     Input  bytes  :                   0
     Output bytes  :                  46
     Input  packets:                   0
     Output packets:                   1
    Local statistics:
     Input  bytes  :                   0
     Output bytes  :                  46
     Input  packets:                   0
     Output packets:                   1
    Transit statistics:
     Input  bytes  :                   0                  0 bps
     Output bytes  :                   0                  0 bps
     Input  packets:                   0                  0 pps
     Output packets:                   0                  0 pps
    Security: Zone: Null
```

```
    Flow Statistics :
.............................
```

```
user@host> show interfaces ge-0/0/2.2 detail
  Logical interface ge-0/0/2.2 (Index 90) (SNMP ifIndex 549) (Generation 162)
    Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.102 ]  Encapsulation: ENET2
    Tenant Name: TSYS2
    Traffic statistics:
     Input  bytes  :                   0
     Output bytes  :                  46
     Input  packets:                   0
     Output packets:                   1
    Local statistics:
     Input  bytes  :                   0
     Output bytes  :                  46
     Input  packets:                   0
     Output packets:                   1
    Transit statistics:
     Input  bytes  :                   0                    0 bps
     Output bytes  :                   0                    0 bps
     Input  packets:                   0                    0 pps
     Output packets:                   0                    0 pps
    Security: Zone: Null
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :              ..............................
```

SEE ALSO

Tenant System Configuration Overview

Understanding Tenant System Security Profiles (Primary Administrators Only)

IN THIS SECTION

Tenant systems allow you to virtually divide a supported SRX Series Firewall into multiple devices, securing them from intrusion and attacks, and protecting them from faulty conditions outside their own contexts. To protect tenant systems, security resources are configured in a manner similar to how they are configured for a discrete device. However, the primary administrator assigns resources to the tenant systems.

An SRX Series Firewall running tenant systems can be partitioned into tenant systems, an interconnected tenant system, if necessary, and the default primary logical system. When the system is initialized, the primary logical system is created at the root. All system resources are assigned to it, effectively creating a default primary logical system security profile. To distribute security resources across the tenant systems, the primary administrator creates security profiles that specify the resources to be allocated to a tenant system. Only the primary administrator can configure security profiles and bind them to the tenant systems. The tenant system administrator uses these resources for the respective tenant system.

The tenant systems are defined by the resources allocated to them, including security components, interfaces, routing instance, static routes, and dynamic routing protocols. The primary administrator configures the security profiles and assigns them to the tenant systems. You cannot commit a tenant system configuration without a security profile assigned to it.

This topic includes the following sections:

Tenant Systems Security Profiles

The primary administrator can configure and assign a security profile to a specific tenant system or multiple tenant systems. The maximum number of security profiles that can be configured depends on the capacity of an SRX Series Firewall. When the maximum number of security profiles have been created, you need to 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 can bind a single security profile to more than one tenant 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 tenant systems appropriately. You can assign various amounts of a resource to the tenant systems and allow the tenant systems to utilize the resources effectively.

  Security profiles protect against one tenant system exhausting a resource that is required at the same time by other tenant systems. Security profiles protect critical system resources and maintain a better performance among tenant systems when the device is experiencing a heavy traffic flow. Security profiles defend against one tenant system dominating the use of resources and allow the other tenant systems to use the resources effectively.

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

You need to delete the security profile of a tenant system before you can delete the tenant system.

Understanding How the System Assesses Resources Assignment and Use Across the Tenant Systems

To provision a tenant system with security features, the primary administrator configures a security profile that specifies the resource for each security feature:

- A reserved quota that guarantees that the specified resource amount is always available to the tenant system.

- A maximum allowed quota. If a tenant system requires additional resources that exceed the reserved quota, then it can utilize the resources configured for the global maximum amount if the global resources are not allocated to the other tenant systems. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. The tenant systems need to utilize the global resources effectively based on the available 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 primary administrator must configure the appropriate maximum allowed quota values in the security profiles so that the maximum resource usage of a specific tenant system does not negatively impact other tenant systems configured on the device.

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

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 tenant systems. A maximum quota for a resource gives a tenant system greater flexibility through access to a larger amount of that resource, but it constrains the amount of resources available to allocate to other tenant systems.

The following security features resources can be specified in a security profile:

- 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)

    NOTE: IPv6 addresses in IPv6 source pools without PAT are not included in security profiles.

  - 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 tenant system security profile dynamically while the security profile is assigned to other tenant systems. However, to ensure that the system resource quota is not exceeded, the system takes the following actions:

- If a static quota is changed, the system process that maintains the tenant system counts for resources specified in security profiles subsequently reevaluates the security profiles assigned to the profile associated with the static quota. This check identifies the number of resources assigned across all tenant 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 tenant system and bind a security profile to it. They are also performed when you bind a different security profile from the security profile that is currently assigned to it to an existing tenant system (or the primary logical system).

- If a dynamic quota is revised, no check is performed, but the revised 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 explained in Table 33 on page 548 and that address allocation of the resources and 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 maximum amount specified—six zones—is available for the tenant systems. The system maximum number of zones is 10.

The three cases address the configuration across the tenant systems. The three cases verify whether a configuration succeeds or fails when it is committed based on the allocation of zones.

Table 32 on page 547 shows the security profiles and their zone allocations.

Table 32: 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**: The primary administrator dynamically increases the reserved zone count specified in this profile later.

Table 32: Security Profiles Used for Reserved Resource Assessments *(Continued)*

Two Security Profiles Used in the Configuration Cases
primary-logical-system-profile • zones maximum quota = 10 • no reserved quota

Table 33 on page 548 shows three cases that illustrate how the system assesses reserved resources for zones across the tenant systems based on the 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 tenant 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 tenant systems is 12, which is greater than the system maximum resource quota.

Table 33: Reserved Resource Allocation Assessment Across Tenant Systems

Reserved Resource Quota Checks Across Tenant 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 tenant systems: tenant-system-1 and tenant-system-2. • The primary-logical-system-profile profile is used exclusively for the primary logical system. • tenant-system-1 = 4 reserved zones. • tenant-system-2 = 4 reserved zones. • primary-logical-system = 0 reserved zones.

Table 33: Reserved Resource Allocation Assessment Across Tenant Systems *(Continued)*

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

Example: Creating Tenant Systems, Tenant System Administrators, and an Interconnect VPLS Switch

IN THIS SECTION

This example shows how to create tenant systems, tenant system administrators, and an interconnect VPLS switch. Only the primary administrator can create user login accounts for tenant system administrators and interconnect VPLS switch.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall.
- Junos OS Release 18.4R1 and later releases.
  - "VSRX requires 20.1R1 and 16GB of memory." on page 19
- Before you begin creating the tenant systems, tenant system administrators, and an interconnect VPLS switch, read "Tenant Systems Overview" on page 525 to understand how this task fits into the overall configuration process.

Overview

IN THIS SECTION

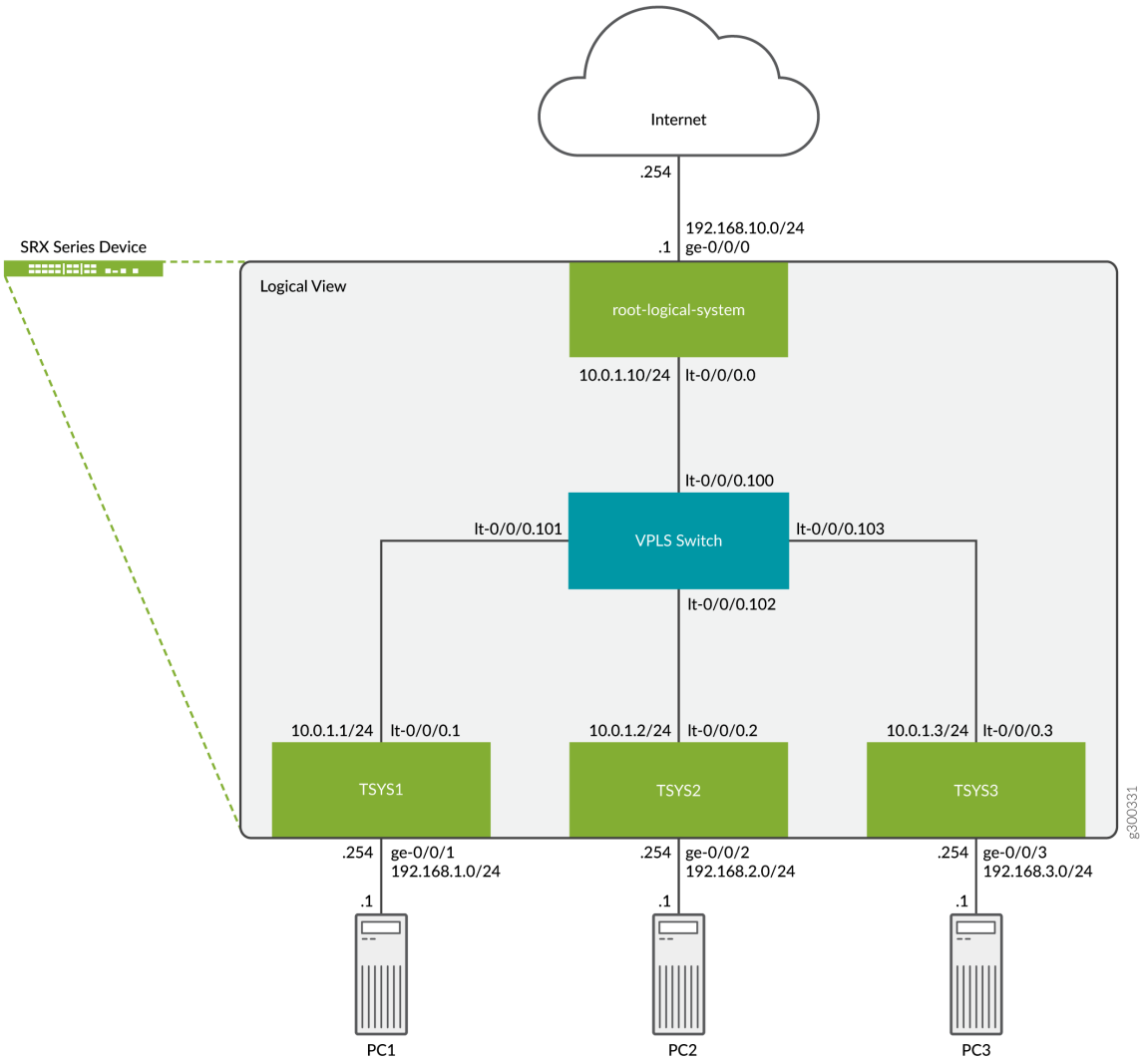
This example shows how to create the tenant systems TSYS1, TSYS2, and TSYS3, and the tenant system administrators for them. You can create multiple tenant system administrators for a tenant system with different permission levels based on your requirements.

This topic also covers the interconnect virtual private LAN service (VPLS) switch connecting one tenant system to another on the same device. The VPLS switch enables both transit traffic and traffic terminated at a tenant system to pass between tenant systems. To allow traffic to pass between tenant systems, logical tunnel (lt-0/0/0) interfaces should be configured in the same subnet.

Topology

The Figure 13 on page 552 shows an SRX Series Firewall deployed and configured for tenant systems. The configuration example uses static routing to allow the PCs to reach the Internet.

Figure 13: Creating Tenant Systems and Interconnect VPLS Switch



Full SRX Quick Configuration

IN THIS SECTION

- Configuring Logical and Tenant Systems, and Interconnect VPLS Switch | 553

CLI Quick Configuration

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

```
set system login class TSYS1admin1 tenant TSYS1
set system login class TSYS1admin1 permissions all
set system login class TSYS2admin1 tenant TSYS2
set system login class TSYS2admin1 permissions all
set system login class TSYS3admin1 tenant TSYS3
set system login class TSYS3admin1 permissions all
set system login user TSYS1admin1 uid 2001
set system login user TSYS1admin1 class TSYS1admin1
set system login user TSYS1admin1 authentication encrypted-password "$ABC123"
set system login user TSYS2admin1 uid 2003
set system login user TSYS2admin1 class TSYS2admin1
set system login user TSYS2admin1 authentication encrypted-password "$ABC123"
set system login user TSYS3admin1 uid 2005
set system login user TSYS3admin1 class TSYS3admin1
set system login user TSYS3admin1 authentication encrypted-password "$ABC123"
set system security-profile SP0 logical-system root-ls
set system security-profile SP1 tenant TSYS1
set system security-profile SP2 tenant TSYS2
set system security-profile SP3 tenant TSYS3
set logical-systems root-ls interfaces ge-0/0/0 unit 0 family inet address 192.168.10.1/24
set logical-systems root-ls interfaces lt-0/0/0 unit 0 encapsulation ethernet
set logical-systems root-ls interfaces lt-0/0/0 unit 0 peer-unit 100
set logical-systems root-ls interfaces lt-0/0/0 unit 0 family inet address 10.0.1.10/24
set logical-systems root-ls routing-options static route 192.168.1.0/24 next-hop 10.0.1.1
set logical-systems root-ls routing-options static route 192.168.2.0/24 next-hop 10.0.1.2
set logical-systems root-ls routing-options static route 192.168.3.0/24 next-hop 10.0.1.3
set logical-systems root-ls security address-book global address TSYS1 192.168.1.0/24
set logical-systems root-ls security address-book global address TSYS2 192.168.2.0/24
set logical-systems root-ls security address-book global address TSYS3 192.168.3.0/24
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
match source-address TSYS1
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
match source-address TSYS2
```

```
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
match source-address TSYS3
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
match destination-address any
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
match application any
set logical-systems root-ls security policies from-zone trust to-zone untrust policy allow-out
then permit
set logical-systems root-ls security zones security-zone trust host-inbound-traffic system-
services ping
set logical-systems root-ls security zones security-zone trust interfaces lt-0/0/0.0
set logical-systems root-ls security zones security-zone untrust host-inbound-traffic system-
services ping
set logical-systems root-ls security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces lt-0/0/0 unit 1 encapsulation ethernet
set interfaces lt-0/0/0 unit 1 peer-unit 101
set interfaces lt-0/0/0 unit 1 family inet address 10.0.1.1/24
set interfaces lt-0/0/0 unit 2 encapsulation ethernet
set interfaces lt-0/0/0 unit 2 peer-unit 102
set interfaces lt-0/0/0 unit 2 family inet address 10.0.1.2/24
set interfaces lt-0/0/0 unit 3 encapsulation ethernet
set interfaces lt-0/0/0 unit 3 peer-unit 103
set interfaces lt-0/0/0 unit 3 family inet address 10.0.1.3/24
set interfaces lt-0/0/0 unit 100 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 100 peer-unit 0
set interfaces lt-0/0/0 unit 101 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 101 peer-unit 1
set interfaces lt-0/0/0 unit 102 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 102 peer-unit 2
set interfaces lt-0/0/0 unit 103 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 103 peer-unit 3
set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.254/24
set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.254/24
set interfaces ge-0/0/3 unit 0 family inet address 192.168.3.254/24
set routing-instances VPLS instance-type vpls
set routing-instances VPLS interface lt-0/0/0.100
set routing-instances VPLS interface lt-0/0/0.101
set routing-instances VPLS interface lt-0/0/0.102
set routing-instances VPLS interface lt-0/0/0.103
set tenants TSYS1 routing-instances vr1 instance-type virtual-router
set tenants TSYS1 routing-instances vr1 routing-options static route 0.0.0.0/0 next-hop 10.0.1.10
set tenants TSYS1 routing-instances vr1 interface lt-0/0/0.1
set tenants TSYS1 routing-instances vr1 interface ge-0/0/1.0
```

```
set tenants TSYS1 security address-book global address PC1 192.168.1.0/24
set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out match source-
address PC1
set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out match
destination-address any
set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out match
application any
set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out then permit
set tenants TSYS1 security zones security-zone PC1 host-inbound-traffic system-services ping
set tenants TSYS1 security zones security-zone PC1 interfaces ge-0/0/1.0
set tenants TSYS1 security zones security-zone VPLS host-inbound-traffic system-services ping
set tenants TSYS1 security zones security-zone VPLS interfaces lt-0/0/0.1
set tenants TSYS2 routing-instances vr2 instance-type virtual-router
set tenants TSYS2 routing-instances vr2 routing-options static route 0.0.0.0/0 next-hop 10.0.1.10
set tenants TSYS2 routing-instances vr2 interface lt-0/0/0.2
set tenants TSYS2 routing-instances vr2 interface ge-0/0/2.0
set tenants TSYS2 security address-book global address PC2 192.168.2.0/24
set tenants TSYS2 security policies from-zone PC2 to-zone VPLS policy allow-out match source-
address PC2
set tenants TSYS2 security policies from-zone PC2 to-zone VPLS policy allow-out match
destination-address any
set tenants TSYS2 security policies from-zone PC2 to-zone VPLS policy allow-out match
application any
set tenants TSYS2 security policies from-zone PC2 to-zone VPLS policy allow-out then permit
set tenants TSYS2 security zones security-zone PC2 host-inbound-traffic system-services ping
set tenants TSYS2 security zones security-zone PC2 interfaces ge-0/0/2.0
set tenants TSYS2 security zones security-zone VPLS host-inbound-traffic system-services ping
set tenants TSYS2 security zones security-zone VPLS interfaces lt-0/0/0.2
set tenants TSYS3 routing-instances vr3 instance-type virtual-router
set tenants TSYS3 routing-instances vr3 routing-options static route 0.0.0.0/0 next-hop 10.0.1.10
set tenants TSYS3 routing-instances vr3 interface lt-0/0/0.3
set tenants TSYS3 routing-instances vr3 interface ge-0/0/3.0
set tenants TSYS3 security address-book global address PC3 192.168.3.0/24
set tenants TSYS3 security policies from-zone PC3 to-zone VPLS policy allow-out match source-
address PC3
set tenants TSYS3 security policies from-zone PC3 to-zone VPLS policy allow-out match
destination-address any
set tenants TSYS3 security policies from-zone PC3 to-zone VPLS policy allow-out match
application any
set tenants TSYS3 security policies from-zone PC3 to-zone VPLS policy allow-out then permit
set tenants TSYS3 security zones security-zone PC3 host-inbound-traffic system-services ping
set tenants TSYS3 security zones security-zone PC3 interfaces ge-0/0/3.0
```

```
set tenants TSYS3 security zones security-zone VPLS host-inbound-traffic system-services ping
set tenants TSYS3 security zones security-zone VPLS 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 CLI User Guide. We will only be covering the configuration of one tenant for the step-by-step procedure.

1. Create the login user accounts for each tenant. We will only show the steps for creating the tenant `TSYS1` user account.

   a. Create the user login class and assign it to the tenant system.

   ```
   [edit]
   user@SRX# set system login class TSYS1admin1 tenant TSYS1
   ```

   b. Assign a permissions level to the login class, for this example we will use the level `all` which allows full access to the tenant system administrator.

   ```
   [edit]
   user@SRX# set system login class TSYS1admin1 permissions all
   ```

   c. Create a user account and assign it to the class from the previous steps. This will allow the user to login to the tenant system.

   ```
   [edit]
   user@SRX# set system login user TSYS1admin1 class TSYS1admin1
   ```

   d. Create a user login password for the user account.

   ```
   [edit]
   user@SRX# set system login user TSYS1admin1 authentication plain-text-password
   New password: "$ABC123"
   Retype new password: "$ABC123"
   ```

2. Configure the VPLS switch. The VPLS switch enables both transit traffic and traffic terminated at a tenant system to pass between tenant systems with a single logical tunnel. Logical tunnel interfaces should be configured in the same subnet to allow traffic between tenant systems.

a. Configure the logical tunnel interfaces.

```
[edit]
user@SRX# set interfaces lt-0/0/0 unit 100 encapsulation ethernet-vpls
user@SRX# set interfaces lt-0/0/0 unit 100 peer-unit 0
user@SRX# set interfaces lt-0/0/0 unit 101 encapsulation ethernet-vpls
user@SRX# set interfaces lt-0/0/0 unit 101 peer-unit 1
user@SRX# set interfaces lt-0/0/0 unit 102 encapsulation ethernet-vpls
user@SRX# set interfaces lt-0/0/0 unit 102 peer-unit 2
user@SRX# set interfaces lt-0/0/0 unit 103 encapsulation ethernet-vpls
user@SRX# set interfaces lt-0/0/0 unit 103 peer-unit 3
```

b. Configure a routing instance for the VPLS switch and assign the logical tunnel interfaces.

```
[edit]
user@SRX# set routing-instances VPLS instance-type vpls
user@SRX# set routing-instances VPLS interface lt-0/0/0.100
user@SRX# set routing-instances VPLS interface lt-0/0/0.101
user@SRX# set routing-instances VPLS interface lt-0/0/0.102
user@SRX# set routing-instances VPLS interface lt-0/0/0.103
```

3. Configure the tenant systems. We are only showing the configuration for one tenant.

a. Configure the interfaces associated with the tenant.

```
[edit]
user@SRX# set interfaces lt-0/0/0 unit 1 encapsulation ethernet
user@SRX# set interfaces lt-0/0/0 unit 1 peer-unit 101
user@SRX# set interfaces lt-0/0/0 unit 1 family inet address 10.0.1.1/24
user@SRX# set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.254/24
```

b. Configure the tenant, routing instance, static routing and assign the interfaces.

```
[edit]
user@SRX# set tenants TSYS1 routing-instances vr1 instance-type virtual-router
user@SRX# set tenants TSYS1 routing-instances vr1 routing-options static route 0.0.0.0/0
next-hop 10.0.1.10
user@SRX# set tenants TSYS1 routing-instances vr1 interface lt-0/0/0.1
user@SRX# set tenants TSYS1 routing-instances vr1 interface ge-0/0/1.0
```

4. Configure the "security profiles" on page 67. We are only showing the minimal configuration needed to configure logical and tenant systems for this example.

```
[edit]
user@SRX# set system security-profile SP0 logical-system root-ls
user@SRX# set system security-profile SP1 tenant TSYS1
user@SRX# set system security-profile SP2 tenant TSYS2
user@SRX# set system security-profile SP3 tenant TSYS3
```

5. Configure the logical systems. This example using an interconnect VPLS switch requires a logical systems.

   a. Configure the interfaces.

```
[edit]
user@SRX# set logical-systems root-ls interfaces ge-0/0/0 unit 0 family inet address
192.168.10.1/24
user@SRX# set logical-systems root-ls interfaces lt-0/0/0 unit 0 encapsulation ethernet
user@SRX# set logical-systems root-ls interfaces lt-0/0/0 unit 0 peer-unit 100
user@SRX# set logical-systems root-ls interfaces lt-0/0/0 unit 0 family inet address
10.0.1.10/24
```

   b. Configure the static routes.

```
[edit]
user@SRX# set logical-systems root-ls routing-options static route 192.168.1.0/24 next-hop
10.0.1.1
user@SRX# set logical-systems root-ls routing-options static route 192.168.2.0/24 next-hop
10.0.1.2
user@SRX# set logical-systems root-ls routing-options static route 192.168.3.0/24 next-hop
10.0.1.3
```

6. Configure security zones and policies in the logical systems to allow traffic flow from the tenants to the Internet. Additional security policies can be configured on both the logical and tenant systems to allow traffic between tenants.

   a. Configure security zones.

```
[edit]
user@SRX# set logical-systems root-ls security zones security-zone trust host-inbound-
```

```
traffic system-services ping
user@SRX# set logical-systems root-ls security zones security-zone trust interfaces
lt-0/0/0.0
user@SRX# set logical-systems root-ls security zones security-zone untrust host-inbound-
traffic system-services ping
user@SRX# set logical-systems root-ls security zones security-zone untrust interfaces
ge-0/0/0.0
```

b. Configure security policies.

```
[edit]
user@SRX# set logical-systems root-ls security address-book global address TSYS1
192.168.1.0/24
user@SRX# set logical-systems root-ls security address-book global address TSYS2
192.168.2.0/24
user@SRX# set logical-systems root-ls security address-book global address TSYS3
192.168.3.0/24
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out match source-address TSYS1
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out match source-address TSYS2
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out match source-address TSYS3
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out match destination-address any
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out match application any
user@SRX# set logical-systems root-ls security policies from-zone trust to-zone untrust
policy allow-out then permit
```

7. Configure security zones and policies in each tenant systems to allow traffic flow to the Internet.

a. Configure security zones.

```
[edit]
user@SRX# set tenants TSYS1 security zones security-zone PC1 host-inbound-traffic system-
services ping
user@SRX# set tenants TSYS1 security zones security-zone PC1 interfaces ge-0/0/1.0
user@SRX# set tenants TSYS1 security zones security-zone VPLS host-inbound-traffic system-
```

```
services ping
user@SRX# set tenants TSYS1 security zones security-zone VPLS interfaces lt-0/0/0.1
```

b. Configure security policies.

```
[edit]
user@SRX# set tenants TSYS1 security address-book global address PC1 192.168.1.0/24
user@SRX# set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out
match source-address PC1
user@SRX# set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out
match destination-address any
user@SRX# set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out
match application any
user@SRX# set tenants TSYS1 security policies from-zone PC1 to-zone VPLS policy allow-out
then permit
```

Results

From configuration mode, confirm your configuration by entering the `show tenants TSYS1` command to verify that the tenant system is created. Enter the `show system login class TSYS1admin1` command to view the permission level for each class that you defined. To ensure that the tenant system administrators are created, enter the `show system login user TSYS1admin1` command. To ensure that the interfaces for interconnect VPLS switch are created, enter the `show interfaces` command. Enter `show logical-systems` to verify the root logical systems configuration.

```
user@SRX# show tenants TSYS1
routing-instances {
    vr1 {
        instance-type virtual-router;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.0.1.10;
            }
        }
        interface lt-0/0/0.1;
        interface ge-0/0/1.0;
    }
}
security {
    address-book {
```

```
        global {
            address PC1 192.168.1.0/24;
        }
    }
    policies {
        from-zone PC1 to-zone VPLS {
            policy allow-out {
                match {
                    source-address PC1;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone PC1 {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone VPLS {
            host-inbound-traffic {
                system-services {
                    ping;
                }
            }
            interfaces {
                lt-0/0/0.1;
            }
        }
```

```
    }
}
```

```
user@SRX# show system login class TSYS1admin1
tenant TSYS1;
permissions all;
```

```
user@SRX# show system login user TSYS1admin1
uid 2001;
class TSYS1admin1;
authentication {
    encrypted-password "$ABC123";
}
```

```
user@SRX# show interfaces
lt-0/0/0 {
    unit 1 {
        encapsulation ethernet;
        peer-unit 101;
        family inet {
            address 10.0.1.1/24;
        }
    }
    unit 2 {
        encapsulation ethernet;
        peer-unit 102;
        family inet {
            address 10.0.1.2/24;
        }
    }
    unit 3 {
        encapsulation ethernet;
        peer-unit 103;
        family inet {
            address 10.0.1.3/24;
        }
    }
    unit 100 {
        encapsulation ethernet-vpls;
```

```
        peer-unit 0;
    }
    unit 101 {
        encapsulation ethernet-vpls;
        peer-unit 1;
    }
    unit 102 {
        encapsulation ethernet-vpls;
        peer-unit 2;
    }
    unit 103 {
        encapsulation ethernet-vpls;
        peer-unit 3;
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.1.254/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 192.168.2.254/24;
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family inet {
            address 192.168.3.254/24;
        }
    }
}
```

```
user@SRX# show logical-systems
root-ls {
    interfaces {
        ge-0/0/0 {
```

```
            unit 0 {
                family inet {
                    address 192.168.10.1/24;
                }
            }
        }
        lt-0/0/0 {
            unit 0 {
                encapsulation ethernet;
                peer-unit 100;
                family inet {
                    address 10.0.1.10/24;
                }
            }
        }
    }
    routing-options {
        static {
            route 192.168.1.0/24 next-hop 10.0.1.1;
            route 192.168.2.0/24 next-hop 10.0.1.2;
            route 192.168.3.0/24 next-hop 10.0.1.3;
        }
    }
    security {
        address-book {
            global {
                address TSYS1 192.168.1.0/24;
                address TSYS2 192.168.2.0/24;
                address TSYS3 192.168.3.0/24;
            }
        }
        policies {
            from-zone trust to-zone untrust {
                policy allow-out {
                    match {
                        source-address [ TSYS1 TSYS2 TSYS3 ];
                        destination-address any;
                        application any;
                    }
                    then {
                        permit;
                    }
                }
```

```
            }
        }
        zones {
            security-zone trust {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
                interfaces {
                    lt-0/0/0.0;
                }
            }
            security-zone untrust {
                host-inbound-traffic {
                    system-services {
                        ping;
                    }
                }
                interfaces {
                    ge-0/0/0.0;
                }
            }
        }
    }
}
```

If the output does not display the intended configuration, repeat the configuration instructions in these examples to correct it. If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying Tenant Systems and Login Configurations Using Primary Administrator

Purpose

Verify that the tenant systems exist and you can enter them from root as the primary administrator. Return from the tenant system to the root.

Action

From operational mode, use the following command to enter the tenant systems TSYS1:

```
user@SRX> set cli tenant TSYS1
Tenant: TSYS1
user@SRX:TSYS1>
```

Now you are entered to the tenant systems TSYS1. Use the following command to exit from tenant systems TSYS1 to the root:

```
user@SRX:TSYS1> clear cli tenant
Cleared default tenants
user@SRX>
```

Meaning

Tenant system exists and you can enter to the tenant system from the root as the primary administrator.

Verifying Tenant Systems and Login Configurations Using SSH

Purpose

Verify that the tenant systems you created exist, and that the administrator login IDs and passwords that you created are correct.

Action

Use SSH to log in to each user tenant system administrator.

1. Run SSH specifying the IP address of your SRX Series Firewall.

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

```
login: TSYS1admin1
Password: "$ABC123"

TSYS1admin1@SRX: TSYS1>
```

Meaning

Tenant system administrator `TSYS1admin1` exists and you can login as the tenant system administrator.

Verifying PC1 Connectivity to the Internet

Purpose

Verify end-to-end connectivity.

Action

Ping and run traceroute to the Internet from PC1. In our example the Internet is 192.168.10.254.

1. Run ping from PC1.

```
user@PC1> ping 192.168.10.254 count 2
PING 192.168.10.254 (192.168.10.254): 56 data bytes
64 bytes from 192.168.10.254: icmp_seq=0 ttl=62 time=3.178 ms
64 bytes from 192.168.10.254: icmp_seq=1 ttl=62 time=3.082 ms

--- 192.168.10.254 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.082/3.130/3.178/0.048 ms
```

2. Run traceroute from PC1.

```
user@PC1> traceroute 192.168.10.254
traceroute to 192.168.10.254 (192.168.10.254), 30 hops max, 52 byte packets
```

```
1  192.168.1.254 (192.168.1.254)  2.188 ms  1.779 ms  1.896 ms
2  10.0.1.10 (10.0.1.10)  1.888 ms  1.535 ms  1.661 ms
3  192.168.10.254 (192.168.10.254)  3.243 ms  15.077 ms  3.499 ms
```

Meaning

PC1 is able to reach the Internet.

SEE ALSO

Session Creation for Devices Running Tenant Systems | 575

Configuring tenant systems Interconnect with Logical Tunnel Interface point-to-point connection | 592

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.2R1	Starting in Junos OS Release 19.2R1, the virtual-router configured in a tenant system is passed as the default routing-instance to `ping`, `telnet`, `ssh`, `traceroute`, `show arp`, `clear arp`, `show ipv6 neighbors`, and `clear ipv6 neighbors` commands.

RELATED DOCUMENTATION

Logical Systems and Tenant Systems support for vSRX Virtual Firewall and vSRX Virtual Firewall 3.0 Instances | 19

Security Zones for Tenant Systems

IN THIS SECTION

Security zones can be configured with tenant systems. For more information see the following topics:

Understanding Zones for Tenant Systems

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

The primary administrator configures the maximum and reserved numbers of security zones for the tenant system. Then the administrator for the tenant system can create the security zones in the tenant system and assign interfaces to each security zone. The number of zones configured in the tenant system count toward the maximum number of zones available on the device. The `show system security-profile zones` command is used to view the number of security zones allocated to the tenant system and the `show interfaces` command to view the interfaces assigned to the tenant system.

You can configure the following features in a tenant system security zone:

- 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 tenant system.

The management functional zone (MGT) can be configured for the tenant system. There is the management interface per device that is allocated to the tenant system.

The administrator for the tenant system can configure and view all attributes for a security zone in a tenant system. All security zone attributes in a tenant system are also visible to the primary administrator.

Example: Configuring Zones in the Tenant System

IN THIS SECTION

This example shows how to configure the zones for the tenant system.

Requirements

Before you begin the configuration:

- Configure the interfaces created by the primary administrator. See *Example: Configuring Interfaces and Routing Instances for a Tenant System*.

Overview

In this example, you can configure zones for the tenant systems. Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. The `[edit tenants tenant-name security zones]` hierarchy level is used to configure the security zones. This example configures the security policies and zones described in Table 34 on page 570.

Table 34: Security Zones Parameters

Feature	Configuration Parameters
Zones 1	• Security zone: trust • System services: any-service • Bind to interfaces xe-0/0/1.0 (trust), xe-0/0/3.0 (untrust)

Table 34: Security Zones Parameters *(Continued)*

Feature	Configuration Parameters
Zone 2	• Security zone: untrust • System services: any-service • Bind to interfaces xe-0/0/1.0 (trust), xe-0/0/3.0 (untrust)

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set tenants TN1 security zones security-zone trust host-inbound-traffic system-services any-service
set tenants TN1 security zones security-zone trust interfaces xe-0/0/1.0
set tenants TN1 security zones security-zone untrust host-inbound-traffic system-services any-service
set tenants TN1 security zones security-zone untrust interfaces xe-0/0/3.0
```

Step-by-Step Procedure

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

To configure security zones in the tenant system:

1. Define the tenant system name as TN1.

```
[edit]
user@host# set tenants TN1
```

2. Configure a security zone as trust that permits traffic from zone trust and assign it to an interface.

```
[edit tenants TN1 security zones security-zone trust]
user@host# set host-inbound-traffic system-services any-service
user@host# set interfaces xe-0/0/1.0
```

3. Configure a security zone as untrust that permits traffic from zone untrust and assign it to an interface.

```
[edit tenants TN1 security zones security-zone untrust]
user@host# set host-inbound-traffic system-services any-service
user@host# set interfaces xe-0/0/3.0
```

Results

From configuration mode, confirm your configuration by entering the `show tenants tenant-name security policies` and `show tenants tenant-name security zones` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TN1 security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            any-service;
        }
    }
    interfaces {
        xe-0/0/1.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
```

```
        system-services {
            any-service;
        }
    }
    interfaces {
        xe-0/0/3.0;
    }
}
```

Verification

IN THIS SECTION

- Verifying Zone Configuration | 573

To confirm that the configuration is working properly, perform the following task:

Verifying Zone Configuration

Purpose

Verify the information about security zones.

Action

To verify the configuration is working properly, enter the `show security zones tenant all` command from operational mode.

```
user@host> show security zones tenant all
```

```
  Tenant: TN1

  Security zone: Host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
```

```
Interfaces:

Security zone: abc
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 0
Interfaces:xe-0/0/1.0

Security zone: def
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Interfaces bound: 1
Interfaces:xe-0/0/3.0
```

Meaning

The output displays the information of security zones configured on the tenant system.

RELATED DOCUMENTATION

Security Policies for Tenant Systems | 650

Flow for Tenant Systems

IN THIS SECTION

This topic explains how packets are processed in flow sessions on devices that are configured with tenant systems. It describes how the device running tenant systems handles pass-through traffic

between tenant systems. This topic also covers self-traffic as self-initiated traffic within a tenant system and self-traffic terminated on another tenant system. Before addressing tenant systems, the topic provides basic information about the SRX Series architecture with respect to packet processing and sessions. Finally, addresses the sessions and how to change session characteristics.

Session Creation for Devices Running Tenant Systems

IN THIS SECTION

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 a traffic enters a tenant system interface, route lookup is performed to identify the next hop interface, and policy lookup is performed.

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

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

Understanding Packet Classification

The Packet classification for a flow-based processing is based on both the physical interface and the *logical interface* and depends on the incoming interface. The packet classification is performed at the ingress point and within a flow, the packet-based processing also takes place on an SPU sometimes.

Packet classification is assessed the same way for devices that are configured with or without tenant systems. The traffic for a dedicated interface is classified to the tenant system that contains that interface. The filters and class-of-service features are typically associated with an interface to influence which packets are allowed to transit the device and to apply special actions to packets as needed.

Understanding the VPLS Switch and Logical Tunnel Interfaces

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

A device running tenant systems can use an internal VPLS switch to pass traffic without it leaving the device. For communication between tenant systems on the device to occur, you must configure an lt-0/0/0 interface on each tenant system that will use the internal switch, and you must associate it with its peer lt-0/0/0 interface on the interconnect tenant system, effectively creating a logical tunnel between them. You define a peer relationship at each end of the tunnel when you configure the tenant system's lt-0/0/0 interfaces.

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

WARNING: If you configure an lt-0/0/0 interface in any tenant system and you do not configure a VPLS switch containing a peer lt-0/0/0 interface for it, the commit will fail.

An SRX Series Firewall running tenant systems can be used in a *chassis cluster* and each node has the same configuration.

When you use SRX Series Firewalls configured with tenant systems within a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. tenant systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

Handling Pass-Through Traffic for Tenant Systems

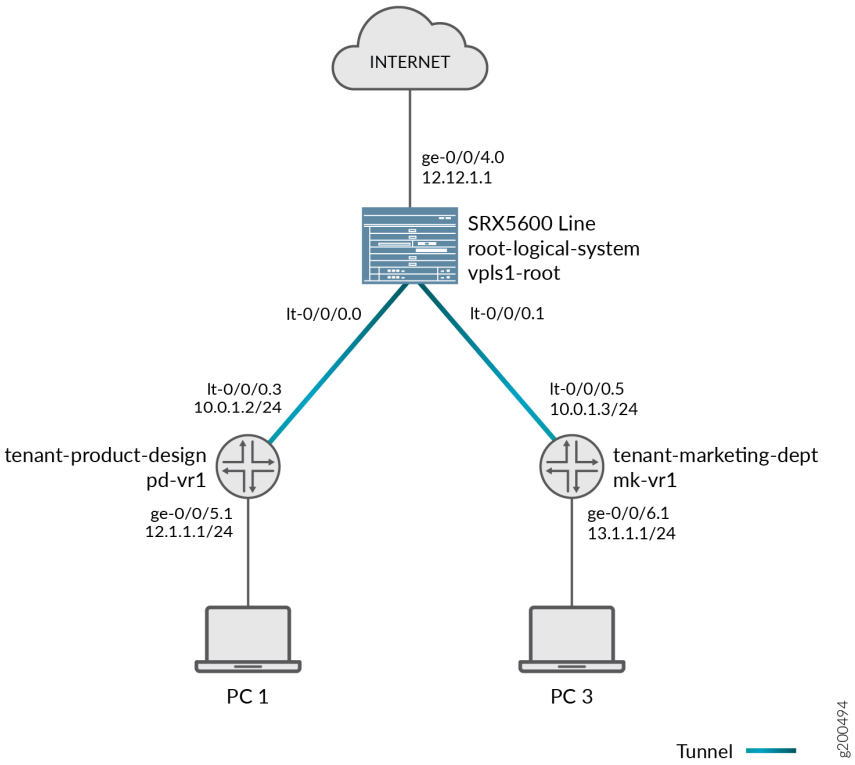
For SRX Series Firewalls running tenant systems, pass-through traffic can exist within a tenant system or between tenant systems.

Pass-Through Traffic Between Tenant Systems

Pass-through traffic between tenant systems is complicated by fact that each tenant 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. Consider how pass-through traffic is handled between tenant systems given in the topology shown in Figure 14 on page 577.

Figure 14: Tenant Systems, Their Virtual Routers, and Their Interfaces



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

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

Consider how pass-through traffic is handled across tenant systems in the topology shown in Figure 14 on page 577.

- A session is established in the incoming tenant system.
  - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the tenant-product-design tenant 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 tenant-marketing-dept.
  - A session is established between ge-0/0/5 and lt-0/0/0.3.
- A session is established in the outgoing tenant system.
  - The packet is injected into the flow again from lt-0/0/0.5, and the tenant system context identified as tenant-marketing-dept is derived from the interface.
  - Packet processing continues in the tenant-marketing-dept tenant 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 tenant system on a device and is either sent out to the network from that tenant system or is terminated on another tenant system on the device.

Self-Initiated Traffic

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

The following process occurs:

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

Consider how self-initiated traffic is handled across tenant systems given the topology shown in Figure 14 on page 577.

- A packet is generated in the tenant-product-design tenant system, and a process for handling the traffic is started in the tenant system.
- Route lookup is performed in pd-vr2, and the egress interface is identified 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 Tenant System

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

- For terminated self-traffic, two policy lookups are performed, and two sessions are established.
  - On the incoming tenant 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 tenant system, another session is set up between the ingress interface (the lt-0/0/0 interface of the second tenant system) and the local interface.

Consider how terminated self-traffic is handled across tenant systems in the topology shown in Figure 14 on page 577.

- A session is established in the incoming tenant system.
  - When a packet arrives on interface ge-0/0/5, it is identified as belonging to the tenant-product-design tenant 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 tenant system.
  - The packet is injected into the flow again from lt-0/0/0.5, and the tenant system context identified as tenant-marketing-dept is derived from the interface.
  - Packet processing continues in the tenant-marketing-dept tenant system.
  - Route lookup for the packet is performed in the mk-vr1 routing instance. The packet is terminated in the destination tenant system as self-traffic.

Understanding Session and Gate Limitation Control

Sessions are created based on routing and other classification information to store information and allocate resources for a flow. The tenant systems flow module provides session and gate limitation to

ensure that these resources are shared among the tenant systems. Resources allocation and limitations for each tenant system are specified in the security profile bound to the tenant system.

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

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.

Configuring Logical Systems and Tenant Systems Interconnect with Multiple VPLS Switches

IN THIS SECTION

This example shows how to interconnect logical systems and tenant systems with multiple VPLS switches. This is achieved by configuring multiple logical systems and tenant systems with more than one logical tunnel (LT) interface under a tenant system and multiple VPLS switches that are configured to pass the traffic without leaving an SRX Series Firewall.

Requirements

This example uses an SRX Series Firewall running Junos OS with logical systems and tenant systems.

Overview

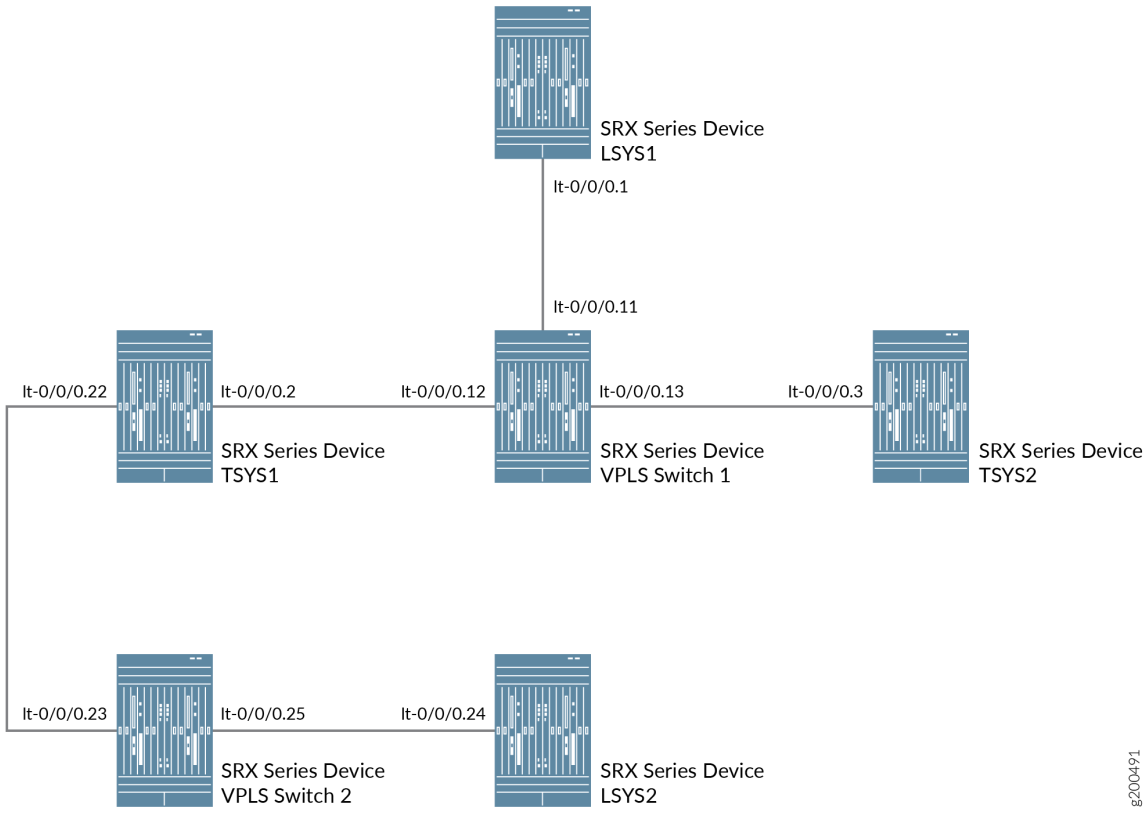
In this example, we configure multiple LT interfaces and multiple VPLS switches under one tenant system.

In this example, we also configure interconnection between multiple logical systems and tenant systems with LT interface point-to point connections (Encapsulation Ethernet and Encapsulation Frame-Relay).

For interconnected logical systems and tenant systems with multiple VPLS switches, this example configures logical tunnel interfaces lt-0/0/0 with ethernet-vpls as the encapsulation type. The corresponding peer lt-0/0/0 interfaces and security-profiles are assigned to the logical systems and tenant systems. The routing instance for the VPLS switch-1 and VPLS switch-2 are also assigned to the logical systems and tenant systems.

Figure 15 on page 582 shows the topology for interconnected logical systems and tenant systems with multiple VPLS switches.

Figure 15: Configuring the interconnected logical systems and tenant systems with multiple VPLS switches.



Configuration

IN THIS SECTION

To configure interfaces for the logical system and tenant system, perform these tasks:

CLI Quick Configuration

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

```
set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 11 peer-unit 1
set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 12 peer-unit 2
set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 13 peer-unit 3
set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 23 peer-unit 22
set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
set interfaces lt-0/0/0 unit 25 peer-unit 24
set routing-instances vpls-switch-1 instance-type vpls
set routing-instances vpls-switch-1 interface lt-0/0/0.11
set routing-instances vpls-switch-1 interface lt-0/0/0.12
set routing-instances vpls-switch-1 interface lt-0/0/0.13
set routing-instances vpls-switch-2 instance-type vpls
set routing-instances vpls-switch-2 interface lt-0/0/0.23
set routing-instances vpls-switch-2 interface lt-0/0/0.25
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address 192.168.0.1/24
set interfaces lt-0/0/0 unit 2 encapsulation ethernet
set interfaces lt-0/0/0 unit 2 peer-unit 12
set interfaces lt-0/0/0 unit 2 family inet address 192.168.0.2/24
set interfaces lt-0/0/0 unit 22 encapsulation ethernet
set interfaces lt-0/0/0 unit 22 peer-unit 23
set interfaces lt-0/0/0 unit 22 family inet address 192.168.4.1/30
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.2
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.22
set interfaces lt-0/0/0 unit 3 encapsulation ethernet
set interfaces lt-0/0/0 unit 3 peer-unit 13
set interfaces lt-0/0/0 unit 3 family inet address 192.168.0.3/24
set tenants TSYS2 routing-instances vr12 instance-type virtual-router
set tenants TSYS2 routing-instances vr12 interface lt-0/0/0.3
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 encapsulation ethernet
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 peer-unit 25
```

```
set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 family inet address 192.168.4.2/30
set system security-profile SP-user policy maximum 100
set system security-profile SP-user policy reserved 50
set system security-profile SP-user zone maximum 60
set system security-profile SP-user zone reserved 10
set system security-profile SP-user flow-session maximum 100
set system security-profile SP-user flow-session reserved 50
set system security-profile SP-user logical-system LSYS1
set system security-profile SP-user tenant TSYS1
set system security-profile SP-user tenant TSYS2
set system security-profile SP-user logical-system LSYS2
```

Procedure

Step-by-Step Procedure

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

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

```
[edit]
user@host# set interfaces lt-0/0/0 unit 11 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 11 peer-unit 1
user@host# set interfaces lt-0/0/0 unit 12 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 12 peer-unit 2
user@host# set interfaces lt-0/0/0 unit 13 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 13 peer-unit 3
user@host# set interfaces lt-0/0/0 unit 23 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 23 peer-unit 22
user@host# set interfaces lt-0/0/0 unit 25 encapsulation ethernet-vpls
user@host# set interfaces lt-0/0/0 unit 25 peer-unit 24
```

2. Configure the routing instance for the VPLS switches and add interfaces to it.

```
[edit]
user@host# set routing-instances vpls-switch-1 instance-type vpls
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.11
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.12
user@host# set routing-instances vpls-switch-1 interface lt-0/0/0.13
```

```
user@host# set routing-instances vpls-switch-2 instance-type vpls
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.23
user@host# set routing-instances vpls-switch-2 interface lt-0/0/0.25
```

3. Configure LSYS1 with lt-0/0/0.1 interface and peer lt-0/0/0.11.

```
[edit]
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 encapsulation ethernet
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 peer-unit 11
user@host# set logical-systems LSYS1 interfaces lt-0/0/0 unit 1 family inet address
192.168.0.1/24
```

4. Configure TSYS1 with lt-0/0/0.2 interface and peer lt-0/0/0.12.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 2 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 2 peer-unit 12
user@host# set interfaces lt-0/0/0 unit 2 family inet address 192.168.0.2/24
user@host# set interfaces lt-0/0/0 unit 22 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 22 peer-unit 23
user@host# set interfaces lt-0/0/0 unit 22 family inet address 192.168.4.1/30
user@host# set tenants TSYS1 routing-instances vr11 instance-type virtual-router
user@host# set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.2
user@host# set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.22
```

5. Configure TSYS2 with lt-0/0/0.3 interface and peer lt-0/0/0.13

```
[edit]
user@host# set interfaces lt-0/0/0 unit 3 encapsulation ethernet
user@host# set interfaces lt-0/0/0 unit 3 peer-unit 13
user@host# set interfaces lt-0/0/0 unit 3 family inet address 192.168.0.3/24
user@host# set tenants TSYS2 routing-instances vr12 instance-type virtual-router
user@host# set tenants TSYS2 routing-instances vr12 interface lt-0/0/0.3
```

6. Configure LSYS2 with lt-0/0/0 interface and peer-unit 24.

```
[edit]
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 encapsulation ethernet
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 peer-unit 25
```

```
user@host# set logical-systems LSYS2 interfaces lt-0/0/0 unit 24 family inet address
192.168.4.2/30
```

7. Assign security-profile for logical-systems.

```
[edit]
user@host# set system security-profile SP-user policy maximum 100
user@host# set system security-profile SP-user policy reserved 50
user@host# set system security-profile SP-user zone maximum 60
user@host# set system security-profile SP-user zone reserved 10
user@host# set system security-profile SP-user flow-session maximum 100
user@host#set system security-profile SP-user flow-session reserved 50
user@host# set system security-profile SP-user logical-system LSYS1
user@host# set system security-profile SP-user tenant TSYS1
user@host# set system security-profile SP-user tenant TSYS2
user@host# set system security-profile SP-user logical-system LSYS2
```

Results

- From configuration mode, confirm your configuration by entering the `show interfaces lt-0/0/0`, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it

```
unit 2 {
    encapsulation ethernet;
    peer-unit 12;
    family inet {
        address 192.168.0.2/24;
    }
}
unit 3 {
    encapsulation ethernet;
    peer-unit 13;
    family inet {
        address 192.168.0.3/24;
    }
}
unit 11 {
    encapsulation ethernet-vpls;
    peer-unit 1;
```

```
}
unit 12 {
    encapsulation ethernet-vpls;
    peer-unit 2;
}
unit 13 {
    encapsulation ethernet-vpls;
    peer-unit 3;
}
unit 22 {
    encapsulation ethernet;
    peer-unit 23;
    family inet {
        address 192.168.4.1/30;
    }
}
unit 23 {
    encapsulation ethernet-vpls;
    peer-unit 22;
}
unit 25 {
    encapsulation ethernet-vpls;
    peer-unit 24;
}
```

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

```
[edit]
user@host# show routing-instances
vpls-switch-1 {
    instance-type vpls;
    interface lt-0/0/0.11;
    interface lt-0/0/0.12;
    interface lt-0/0/0.13;
}
vpls-switch-2 {
    instance-type vpls;
    interface lt-0/0/0.23;
```

```
    interface lt-0/0/0.25;
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS1`, 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 LSYS1
interfaces {
    lt-0/0/0 {
        unit 1 {
            encapsulation ethernet;
            peer-unit 11;
            family inet {
                address 192.168.0.1/24;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2`, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS1
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.2;
        interface lt-0/0/0.22;
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS3`, command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS2
routing-instances {
    vr12 {
        instance-type virtual-router;
        interface lt-0/0/0.3;
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS2`, 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 LSYS2
interfaces {
    lt-0/0/0 {
        unit 24 {
            encapsulation ethernet;
            peer-unit 25;
            family inet {
                address 192.168.4.2/30;
            }
        }
    }
}
```

- 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 configuration instructions in this example to correct it.

```
[edit]
user@host# show system security-profile
SP-user {
    policy {
        maximum 100;
```

```
        reserved 50;
    }
    zone {
        maximum 60;
        reserved 10;
    }
    flow-session {
        maximum 100;
        reserved 50;
    }
    logical-system [ LSYS1 LSYS2 ];
    tenant [ TSYS1 TSYS2 ];
}
```

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

Verification

IN THIS SECTION

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

Verifying the Security-Profile for Logical-systems

Purpose

Verify security profile for each logical systems.

Action

From operational mode, enter the `show system security-profile security-log-stream-number logical-system all` command.

```
user@host> show system security-profile assignment summary
```

```
                                  Total     Maximum
security-profiles                     1          65
logical-systems                       1          32
tenants                               0          32
logical-systems and tenants           1          64
```

Meaning

The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Verifying the LT Interfaces for Logical systems

Purpose

Verify interfaces for logical systems.

Action

From operational mode, enter the `show interfaces lt-0/0/0 terse` command.

```
user@host> show interfaces lt-0/0/0 terse
```

```
Interface               Admin Link Proto    Local                 Remote
lt-0/0/0                up    up
lt-0/0/0.1              up    up   inet     192.168.0.1/24
lt-0/0/0.2              up    up   inet     192.168.0.2/24
lt-0/0/0.3              up    up   inet     192.168.0.3/24
lt-0/0/0.11             up    up   vpls
lt-0/0/0.12             up    up   vpls
```

```
lt-0/0/0.13             up    up   vpls
lt-0/0/0.22             up    up   inet     192.168.4.1/30
lt-0/0/0.23             up    up   vpls
lt-0/0/0.24             up    up   inet     192.168.4.2/30
lt-0/0/0.25             up    up   vpls
lt-0/0/0.32767          up    up
```

Meaning

The output provides the status of LT interfaces. All the LT interfaces are up.

Configuring tenant systems Interconnect with Logical Tunnel Interface point-to-point connection

IN THIS SECTION

This example shows how to interconnect tenant systems with logical tunnel (LT) interfaces in a point-to-point connection.

Requirements

This example uses an SRX Series Firewall running Junos OS with logical systems and tenant systems.

Overview

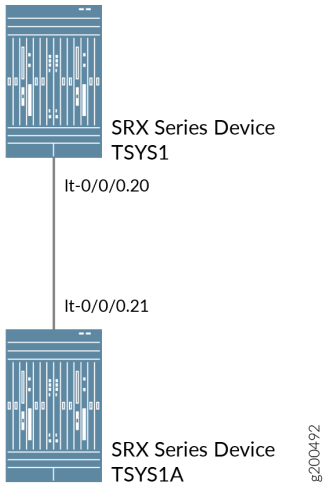
In this example we show how to interconnect tenant systems with logical tunnel (LT) interface in a point-to-point connection.

For the interconnected tenant systems with a point-to-point connection (encapsulation frame-relay) LT interface, this example configures the logical tunnel interface lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems.

The interconnected logical system lt-0/0/0 interface is configured with frame-relay as the encapsulation type. The corresponding peer lt-0/0/0 interfaces in the tenant systems are configured with frame-relay as the encapsulation type. A security profile is assigned to the tenant systems.

Figure 16 on page 593 shows the topology for interconnected tenant systems with a point-to-point connection LT interface.

Figure 16: Configuring the interconnect tenant systems with a point-to-point connection LT interface



Configuration

IN THIS SECTION

To configure security-zone and assigns interfaces to tenant systems, perform these tasks:

CLI Quick Configuration

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

```
set system security-profile sp1 tenant TSYS1
set system security-profile sp2 tenant TSYS1A
set interfaces xe-0/0/5 gigether-options redundant-parent reth0
set interfaces xe-0/0/6 gigether-options redundant-parent reth1
set interfaces xe-1/0/5 gigether-options redundant-parent reth0
set interfaces xe-1/0/6 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 2
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces lt-0/0/0 unit 20 encapsulation ethernet
set interfaces lt-0/0/0 unit 20 peer-unit 21
set interfaces lt-0/0/0 unit 20 family inet address 198.51.1.20/24
set interfaces reth0 unit 0 family inet address 198.51.100.1/24
set interfaces lt-0/0/0 unit 21 encapsulation ethernet
set interfaces lt-0/0/0 unit 21 peer-unit 20
set interfaces lt-0/0/0 unit 21 family inet address 198.51.1.21/24
set interfaces reth1 unit 0 family inet address 192.0.2.1/24
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.20
set tenants TSYS1 routing-instances vr11 interface reth0.0
set tenants TSYS1 routing-instances vr11 routing-options static route 192.0.2.0/24 next-hop
198.51.1.21
set tenants TSYS1 security policies default-policy permit-all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic system-services all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone trust interfaces reth0.0
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic system-services all
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone untrust interfaces lt-0/0/0.20
set tenants TSYS1A routing-instances vr12 instance-type virtual-router
set tenants TSYS1A routing-instances vr12 interface lt-0/0/0.21
set tenants TSYS1A routing-instances vr12 interface reth1.0
set tenants TSYS1A routing-instances vr12 routing-options static route 198.51.100.0/24 next-hop
198.51.1.20
set tenants TSYS1A security policies default-policy permit-all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic system-services all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic protocols all
```

```
set tenants TSYS1A security zones security-zone trust interfaces reth1.0
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic system-services all
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic protocols all
set tenants TSYS1A security zones security-zone untrust interfaces lt-0/0/0.21
```

Configuring [item]

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*.

1. Define a security profile sp1 and assign to a tenant system TNI. Define another security profile sp1 and assign to a tenant system TSYS1A

```
[edit]
user@host# set system security-profile sp1 tenant TSYS1
user@host# set system security-profile sp2 tenant TSYS1A
```

2. Set the interface for reth0 and reth1 and assign it to the redundancy group 1 and redundancy group 2.

```
[edit]
set interfaces xe-0/0/5 gigether-options redundant-parent reth0
set interfaces xe-0/0/6 gigether-options redundant-parent reth1
set interfaces xe-1/0/5 gigether-options redundant-parent reth0
set interfaces xe-1/0/6 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 2
set interfaces reth1 redundant-ether-options redundancy-group 1
```

3. Set the LT interface as encapsulation ethernet in the tenant system TSYS1.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 encapsulation ethernet
```

4. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 peer-unit 21
```

5. Specify the IP address for the LT interface.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 family inet address 198.51.1.20/24
```

6. Specify the IP address for the reth0.

```
[edit]
user@host# set interfaces reth0 unit 0 family inet address 198.51.100.1/24
```

7. Set the LT interface as encapsulation ethernet in the tenant system TSYS1A.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 21 encapsulation ethernet
```

8. Configure a peer unit relationship between LT interfaces, thus creating a point-to-point connection.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 21 peer-unit 20
```

9. Specify the IP address for the LT interface.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 21 family inet address 198.51.1.21/24
```

10. Specify the IP address for the reth1.

```
[edit]
user@host# set interfaces reth1 unit 0 family inet address 192.0.2.1/24
```

11. Define the routing-instances for TSYS1.

```
[edit]
set tenants TSYS1 routing-instances vr11 instance-type virtual-router
set tenants TSYS1 routing-instances vr11 interface lt-0/0/0.20
set tenants TSYS1 routing-instances vr11 interface reth0.0
set tenants TSYS1 routing-instances vr11 routing-options static route 192.0.2.0/24 next-hop
198.51.1.21
```

12. Configure a security policy that permits all traffics.

```
[edit]
user@host# set tenants TSYS1 security policies default-policy permit-all
```

13. Configure security zones.

```
[edit]
set tenants TSYS1 security zones security-zone trust host-inbound-traffic system-services
all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone trust interfaces reth0.0
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic system-services
all
set tenants TSYS1 security zones security-zone untrust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone untrust interfaces lt-0/0/0.20
```

14. Define the routing-instances for TSYS1A.

```
[edit]
set tenants TSYS1A routing-instances vr12 instance-type virtual-router
set tenants TSYS1A routing-instances vr12 interface lt-0/0/0.21
set tenants TSYS1A routing-instances vr12 interface reth1.0
set tenants TSYS1A routing-instances vr12 routing-options static route 198.51.100.0/24 next-
hop 198.51.1.20
```

15. Configure a security policy that permits all traffics.

```
[edit]
set tenants TSYS1A security policies default-policy permit-all
```

16. Configure security zones.

```
[edit]
set tenants TSYS1A security zones security-zone trust host-inbound-traffic system-services
all
set tenants TSYS1A security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1A security zones security-zone trust interfaces reth1.0
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic system-
services all
set tenants TSYS1A security zones security-zone untrust host-inbound-traffic protocols all
set tenants TSYS1A security zones security-zone untrust interfaces lt-0/0/0.21
```

Results

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS1
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.20;
        interface reth0.0;
        routing-options {
            static {
                route 192.0.2.0/24 next-hop 198.51.1.21;
            }
        }
    }
}
security {
    policies {
        default-policy {
```

```
            permit-all;
        }
    }
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                reth0.0;
            }
        }
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lt-0/0/0.20;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1A` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS1A
routing-instances {
    vr12 {
        instance-type virtual-router;
```

```
        interface lt-0/0/0.21;
        interface reth1.0;
        routing-options {
            static {
                route 198.51.100.0/24 next-hop 198.51.1.20;
            }
        }
    }
}
security {
    policies {
        default-policy {
            permit-all;
        }
    }
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                reth1.0;
            }
        }
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lt-0/0/0.21;
            }
        }
```

```
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the Security-Profile for all tenant systems

Purpose

Verify security profile for each logical systems.

Action

From operational mode, enter the `show system security-profile zone tenant al` command.

```
user@host> show system security-profile zone tenant al
```

```
logical-system tenant name   security profile name       usage    reserved     maximum

T1                           bronze                        1           0        2048
T1A                            pX                            0           0        2048
```

Meaning

The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Configuring Logical System and Tenant System Interconnect with a Logical Tunnel Interface point-to-point connection

IN THIS SECTION

This example shows how to interconnect logical systems and tenant systems with logical tunnel (LT) interface in a point-to-point connection.

Requirements

This example uses an SRX Series Firewall running Junos OS with logical systems and tenant systems.

Overview

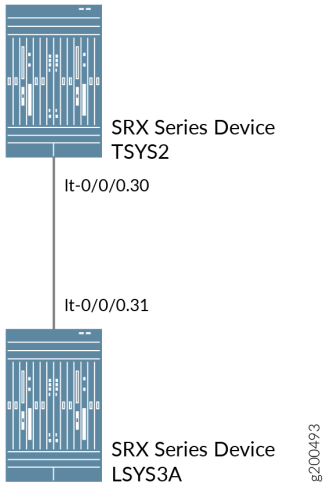
In this example we show how to interconnect logical systems and tenant systems with logical tunnel (LT) interface point-to-point connection.

For the interconnect logical system and tenant system with a point-to-point connection LT interface, the example configures logical tunnel interfaces lt-0/0/0. This example configures security-zone and assigns interfaces to the logical systems

To interconnect the logical system and tenant system, lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. The corresponding peer lt-0/0/0 interfaces are configured with Ethernet as the encapsulation type. A security profile is assigned to the logical system and tenant system

Figure 17 on page 603 shows the topology for interconnected logical systems and tenant systems with LT interface point-to-point connection.

Figure 17: Configuring the interconnect between logical systems and tenant systems with a point-to-point connection LT interface



Configuration

IN THIS SECTION

To configure security-zone and assigns interfaces to logical systems, perform these tasks:

CLI Quick Configuration

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

```
set system security-profile SP-user tenant TSYS2
set interfaces lt-0/0/0 unit 30 encapsulation ethernet
set interfaces lt-0/0/0 unit 30 peer-unit 31
set interfaces lt-0/0/0 unit 30 family inet address 192.255.2.1/30
set tenants TSYS2 routing-instances vr11 instance-type virtual-router
```

```
set tenants TSYS2 routing-instances vr11 interface lt-0/0/0.30
set security zones security-zone LT interfaces lt-0/0/0.30
set system security-profile SP-user logical-system LSYS3A
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 encapsulation ethernet
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 peer-unit 20
set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 family inet address 192.255.2.2/30
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match source-
address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match destination-
address any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT match application
any
set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT then permit
set logical-systems LSYS3A security policies default-policy permit-all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic system-services
all
set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic protocols all
set logical-systems LSYS3A security zones security-zone LT interfaces lt-0/0/0.31
```

Procedure

Step-by-Step Procedure

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

1. Define a security profile and assign to a tenant system.

```
[edit]
user@host# set system security-profile SP-user tenant TSYS2
```

2. Set the LT interface as encapsulation ethernet in the tenant system.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 encapsulation ethernet
```

3. Configure a peer relationship for tenant systems TSYS2.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 peer-unit 21
```

4. Specify the IP address for the LT interface.

```
[edit]
user@host# set interfaces lt-0/0/0 unit 20 family inet address 192.255.2.1/30
```

5. Set the security zone for the LT interface.

```
[edit]
user@host# set logical-systems LSYS2 security zones security-zone LT interfaces lt-0/0/0.30
```

6. Define a security profile and assign to a logical system.

```
[edit]
user@host# set system security-profile SP-user logical-system LSYS3A
```

7. Define the routing-instances for TSYS2.

```
[edit]
set tenants TSYS2 routing-instances vr11 instance-type virtual-router
set tenants TSYS2 routing-instances vr11 interface lt-0/0/0.30
```

8. Set the LT interface as encapsulation ethernet in the logical system 3A.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 encapsulation ethernet
```

9. Configure a peer relationship for logical systems LSYS3A.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 peer-unit 20
```

10. Specify the IP address for the LT interface.

```
[edit]
user@host# set logical-systems LSYS3A interfaces lt-0/0/0 unit 21 family inet address
192.255.2.2/30
```

11. Configure a security policy that permits traffic from the LT zone to the LT policy LT zone.

```
[edit]
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match source-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match destination-address any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
match application any
user@host# set logical-systems LSYS3A security policies from-zone LT to-zone LT policy LT
then permit
```

12. Configure a security policy that permits traffic from default-policy.

```
[edit]
user@host# set logical-systems LSYS3A security policies default-policy permit-all
```

13. Configure security zones.

```
[edit]
user@host# set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
system-services all
user@host# set logical-systems LSYS3A security zones security-zone LT host-inbound-traffic
protocols all
user@host# set logical-systems LSYS3A security zones security-zone LT interfaces
lt-0/0/0.31
```

Results

- From configuration mode, confirm your configuration by entering the `show tenants TSYS2` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show tenants TSYS2
routing-instances {
    vr11 {
        instance-type virtual-router;
        interface lt-0/0/0.30;
    }
}
```

- From configuration mode, confirm your configuration by entering the `show logical-systems LSYS3A` 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 LSYS3A
interfaces {
    lt-0/0/0 {
        unit 21 {
            encapsulation ethernet;
            peer-unit 20;
            family inet {
                address 192.255.2.2/30;
            }
        }
    }
}
security {
    policies {
        from-zone LT to-zone LT {
            policy LT {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
```

```
                then {
                    permit;
                }
            }
        }
        default-policy {
            permit-all;
        }
    }
    zones {
        security-zone LT {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lt-0/0/0.31;
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the LT Interfaces for all Logical and tenant systems

Purpose

Verify interfaces for logical systems.

Action

From operational mode, enter the `show system security-profile zone all-logical-systems-tenants` command.

```
user@host> show system security-profile zone all-logical-systems-tenants
```

```
logical-system tenant name   security profile name       usage    reserved     maximum

root-logical-system          Default-Profile                1           0        2048
LSYS3A1                        gold                           1           0        2048
TSYS23                          bronze                         1           0        2048
```

Meaning

The output provides the status of LT interfaces. All the LT interfaces are up.

Verifying the Security-Profile for all Logical-systems

Purpose

Verify security profile for each logical systems.

Action

From operational mode, enter the `show system security-profile security-log-stream-number logical-system all` command.

```
user@host> show system security-profile security-log-stream-number logical-system all
```

```
logical system name   security profile name       usage    reserved   maximum
root-logical-system   Default-Profile                2           0          2000
LSYS3A                 SP-user                        1          10          60
```

Meaning

The output provides the usage and reserved values for the logical systems when security-log-stream is configured.

Flow Trace for Tenant Systems

IN THIS SECTION

Flow trace also called traceoptions, allows you to monitor traffic flow into and out of an SRX Series Firewall. You can use tracoptions as debugging tool to trace the packets as they traverse the SRX Series Firewall. Traceoptions help you to get details of actions by your security device.

Flow Trace Support for Tenant Systems Overview

For an SRX Series Firewall configured with tenant systems, by default the traceoptions are configured at the root level only. In this case, all the system traces including root and tenant systems are logged in one single trace file. This generated large amounts of information in a single file.

Starting in Junos OS Release 19.4R1, you can enable tracing operations per tenant system level. When you configure the traceoptions at the tenant system level, then the traces for that specific tenant systems are logged in the respective trace file. You can generate an output file for the specified tenant system, and you can find the required traffic information easily in the trace file.

When you enable traceoptions, you specify the name of the file and the type of information you want to trace.

All flow trace sent to one log file in root, if you enable the traceoptions under root context. Traces for a tenant system only sent to the respective trace file, if you enable the traceoptions for the specific tenant system.

Configure Flow Trace Support for Tenant Systems

Configuring traceoptions for a tenant system includes configuring both a target file and a flag. The target file determines where the trace output is recorded. The flag defines what type of data to be collected. If you configure traceoptions for a tenant system, the respective trace file sent to the specific tenant system log file only.

To configure traceoptions for a tenant system:

1. Create tenant system `TSYS1` and setup the basic configurations. See "Tenant System Configuration Overview" on page 533.
2. Configure target file to save the trace information for the tenant system.

```
[edit]
user@host# set tenants TSYS1 security flow traceoptions file flow_tsys1.log
user@host# set tenants TSYS1 security flow traceoptions file size 1g
```

3. Configure traceoptions flag for the tenant system.

```
[edit]
user@host# set tenants TSYS1 security flow traceoptions flag all
```

After you commit the traceoptions configuration, you can view the traceoptions debug files for the tenant system using `show log` *`tracefilename`* operational command.

```
user@host:TSYS1> show log flow_tsys1.logNov  7 13:21:47
13:21:47.217744:CID-0:THREAD_ID-05:LSYS_ID-32:RT:<192.0.2.0/0->198.51.100.0/9011;1,0x0> :

Nov  7 13:21:47 13:21:47.217747:CID-0:THREAD_ID-05:LSYS_ID-32:RT:packet [84] ipid = 39281,
@0x7f490ae56d52

Nov  7 13:21:47 13:21:47.217749:CID-0:THREAD_ID-05:LSYS_ID-32:RT:---- flow_process_pkt: (thd 5):
flow_ctxt type 0, common flag 0x0, mbuf 0x4882b600, rtbl7

Nov  7 13:21:47 13:21:47.217752:CID-0:THREAD_ID-05:LSYS_ID-32:RT: flow process pak fast ifl 88
in_ifp lt-0/0/0.101

Nov  7 13:21:47 13:21:47.217753:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  lt-0/0/0.101:192.0.2.0-
>198.51.100.0, icmp, (0/0)

Nov  7 13:21:47 13:21:47.217756:CID-0:THREAD_ID-05:LSYS_ID-32:RT: find flow: table 0x11d0a2680,
hash 20069(0xffff), sa 192.0.2.0, da 198.51.100.0, sp 0, d0

Nov  7 13:21:47 13:21:47.217760:CID-0:THREAD_ID-05:LSYS_ID-32:RT:Found: session id 0x12. sess
tok 28685

Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow got session.

Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow session id 18

Nov  7 13:21:47 13:21:47.217763:CID-0:THREAD_ID-05:LSYS_ID-32:RT: vector bits 0x200 vector
0x84ae85f0

Nov  7 13:21:47 13:21:47.217764:CID-0:THREAD_ID-05:LSYS_ID-32:RT:set nat 0x11e463550(18) timeout
const to 2

Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT: set_nat_timeout 2 on session 18

Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT:refresh nat 0x11e463550(18)
timeout to 2

Nov  7 13:21:47 13:21:47.217767:CID-0:THREAD_ID-05:LSYS_ID-32:RT:insert usp tag for apps
```

```
Nov  7 13:21:47 13:21:47.217768:CID-0:THREAD_ID-05:LSYS_ID-32:RT:mbuf 0x4882b600, exit nh
0xfffb0006
```

Firewall Authentication for Tenant Systems

IN THIS SECTION

The firewall authentication feature is introduced for tenant systems in Junos OS Release 18.3R1 on the Juniper SRX Series Firewalls to enable you to restrict or permit users individually or in groups. The authentication requests are initiated based on destination addresses defined in the policies.

Understanding Tenant 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.

Firewall authentication is a policy-based authentication method, which requires user to initiate an authentication request through HTTP, FTP or Telnet traffic.

Junos OS enables administrators to restrict and permit firewall users to access protected resources behind a firewall based on their source IP address and other credentials.

The primary administrator configures the following:

- maximum and reserved number of firewall authentication sessions in the tenant system.
- access profile using the profile configuration command at the `[edit access]` hierarchy which is available to all the tenant systems.

Access profiles allows to:

- Storing usernames and passwords of users or point to external authentication servers where such information is stored.
- Including the order of authentication methods, LDAP or RADIUS server options, and session options.
- Associating with a security policy in the tenant system.

After defining the firewall users, create a policy that requires the users to authenticate through one of the authentication modes defined in the Table 35 on page 614.

Table 35: Firewall Authentication Options

Authentication Options	Description	Supported Protocols	Supported Backend
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.	HTTP HTTPS	Local LDAP RADIUS SecurId
Pass-through	Inline authentication with a host or a user from one zone tries to access resources on another zone. The device uses the supported protocols 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.	HTTP HTTPS TELNET FTP	Local LDAP RADIUS SecurId

Table 35: Firewall Authentication Options *(Continued)*

Authentication Options	Description	Supported Protocols	Supported Backend
Web Redirect	Automatically redirect client to WebAuth page for authentication (http or https)	HTTP HTTPS	Local LDAP RADIUS SecurId
Integrated User Firewall	SRX Series devices uses WMI client (WMIC) requests to the AD to get IP address-to-user mapping information in Security event logs.	none	Active Directory
User-Firewall	Same as pass-through but user information is passed to USERID process to go in Auth Table	HTTP HTTPS	Local LDAP RADIUS SecurId

The tenant system administrator configures the following properties for firewall authentication in the tenant 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. In an access profile, users or user groups can be 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.

- The 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.

  Host inbound traffic. Protocols, services, or both are allowed to access the tenant 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.

Configuring Firewall Authentication for a Tenant System

IN THIS SECTION

This example shows how to send different firewall authentication traffic from the client to server across one tenant system using the three authentication modes pass-through, pass-through with web-redirect, and web authentication.

Requirements

This example uses the following hardware and software components:

- an SRX4100 device
- Junos OS Release 18.3R1 and later
- Telnet or HTTP
- External authentication servers are RADIUS, LDAP, and SecurID

Ensure to have the following configured to send firewall authentication traffic from client to server:

- Configure security zones for a tenant system
- Configure interfaces created by the primary administrator

Overview

IN THIS SECTION

When a firewall user attempts to initiate a Telnet, HTTP, or HTTPS session to access a resource in another zone, the SRX Series firewall acts a proxy to authenticate the firewall users before allowing the users to access the Telnet, HTTP, or HTTPS servers behind the firewall.

In this example, you can configure a tenant system and bind the security policy to it. When the traffic from is sent from client to server as referred in Figure 18 on page 618, the users are authenticated based on the authentication process defined in the security policy.

NOTE: The primary administrator is responsible for creating tenants and assigning the system resources such as routing-instances, interfaces in routing-instances and security-profile to tenant system.

Table 36: Firewall Configuration for the Tenant System

Feature	Name	Description
security-profile	tn1_pf	Name of the security profile. This profile specifies the resources to allocate to a tenant system to which the security profile is bound.
interfaces	xe-0/0/1 xe-0/0/2	Name of the interfaces. The interfaces provide traffic connectivity.
access profile	local_pf radius_pf securid_pf	Name of the access profiles. These profiles are used to define the users and passwords and to obtain authorization information about the user's access right.
SSL termination profile	fwauthhttpspf	Name of the profile. This profile is used for SSL termination services.
routing-instances	vr1	Instance type as virtual routing instance.
security policies	p7	Name of the policy. This policy is used to configure pass-through firewall-authentication using fwauthhttpspf SSL termination profile.
	p1	Name of the policy. This policy is used to configure pass-through firewall-authentication using local_pf access profile.

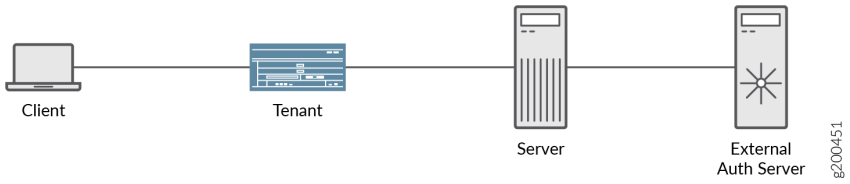
Table 36: Firewall Configuration for the Tenant System *(Continued)*

Feature	Name	Description
	p4	Name of the policy. This policy is used to configure pass-through web-redirect firewall-authentication using radius_pf.
	p3	Name of the policy. This policy is used to configure web-authentication firewall-authentication.

Topology

Figure 18 on page 618 shows the topology used in this configuration example. The tenant shown in this topology is an SRX Series Firewall partitioned to multiple tenants. The external servers supported are RADIUS, LDAP, and SecurID. The communication from the client to the tenant happens over xe-0/0/1 interface and from the tenant to the server happens over xe-0/0/2 interface.

Figure 18: Topology for Tenant System



Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set system security-profile tn1_pf policy maximum 500
set system security-profile tn1_pf policy reserved 100
set system security-profile tn1_pf zone maximum 50
set system security-profile tn1_pf zone reserved 10
set tenants tn1 security-profile tn1_pf
set services ssl termination profile fwauthhttpspf server-certificate device
set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.0/24
set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.254/16 web-authentication http
set interfaces xe-0/0/2 unit 0 family inet address 198.51.100.0/24 web-authentication http
set access profile local_pf client test firewall-user password "$ABC123"
set access profile local_pf client test1 client-group local-group1
set access profile local_pf client test1 client-group local-group2
set access profile local_pf client test1 firewall-user password "$BCD678"
set access profile local_pf client test2 client-group local-group2
set access profile local_pf client test2 firewall-user password "$DEF234"
set access profile local_pf client test3 client-group local-group3
set access profile local_pf client test3 firewall-user password "$DBC123"
set access profile local_pf client test4 client-group local-group4
set access profile local_pf client test4 firewall-user password "$FAB123"
set access profile radius_pf authentication-order radius
set access profile radius_pf radius-server 203.0.113.1 secret "$AFD123"
set access profile securid_pf authentication-order securid
set tenants tn1 routing-instances vr1 instance-type virtual-router
set tenants tn1 routing-instances vr1 interface xe-0/0/1.0
set tenants tn1 routing-instances vr1 interface xe-0/0/2.0
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match source-
address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match
destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 match
application junos-telnet
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p1 then permit
firewall-authentication pass-through access-profile local_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match source-
address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match
```

```
destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 match
application any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 then permit
firewall-authentication pass-through access-profile local_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p7 then permit
firewall-authentication pass-through ssl-termination-profile fwauthhttpspf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match source-
address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match
destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 match
application junos-http
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 then permit
firewall-authentication pass-through access-profile radius_pf
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p4 then permit
firewall-authentication pass-through web-redirect
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match source-
address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match
destination-address any
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 match
application junos-http
set tenants tn1 security policies from-zone tn1_trust to-zone tn1_untrust policy p3 then permit
firewall-authentication web-authentication
set tenants tn1 security policies policy-rematch
set tenants tn1 security zones security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-
traffic system-services all
set tenants tn1 security zones security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-
traffic protocols all
set tenants tn1 security zones security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-
traffic system-services all
set tenants tn1 security zones security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-
traffic protocols all
set tenants tn1 access firewall-authentication pass-through default-profile local_pf
set tenants tn1 access firewall-authentication pass-through telnet banner login
****tenant1_telnet_login_banner
set tenants tn1 access firewall-authentication pass-through telnet banner success
****tenant1_telnet_success_banner
set tenants tn1 access firewall-authentication pass-through telnet banner fail
****tenant1_telnet_fail_banner
set tenants tn1 access firewall-authentication web-authentication default-profile securid_pf
```

```
set tenants tn1 access firewall-authentication web-authentication banner success
****tenant1_webauth_success_banner
```

Configuring access profiles and firewall authentication

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.

1. Configure a security profile tn1_pf and bind it to the tenant system.

```
[edit system security-profile]
user@host# set tn1_pf policy maximum 500
user@host# set tn1_pf policy reserved 100
user@host# set tn1_pf zone maximum 50
user@host# set tn1_pf zone reserved 10
```

2. Create a tenant system tn1 and bind the security profile tn1_pf to the tenant system.

```
[edit tenants]
user@host# set tn1 security-profile tn1_pf
```

3. Define the access profile used for SSL termination services for HTTPS traffic to trigger pass-through authentication.

```
[edit services]
user@host# set ssl termination profile fwauthhttpspf server-certificate device
```

4. Configure interfaces and assign IP addresses. Enable web authentication at xe-0/0/1 interface.

```
[edit interfaces]
user@host# set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces xe-0/0/1 unit 0 family inet address 192.0.2.254/24 web-
authentication http
user@host# set interfaces xe-0/0/2 unit 0 family inet address 198.51.100.0/24 web-
authentication http
```

5. Configure routing instances and add interfaces to it.

```
[edit tenants tn1 routing-instances]
user@host# set vr1 instance-type virtual-router
user@host# set vr1 interface xe-0/0/1.0
user@host# set vr1 interface xe-0/0/2.0
```

Step-by-Step Procedure

The primary administrator is responsible for configuring access profiles in the tenant system. To configure access profiles:

1. Create the access profiles to be used for firewall authentication. Access profiles defines clients as firewall users and the passwords that provide them access for firewall authentication. When unauthenticated traffic is permitted for firewall authentication, the user is authenticated based on the access profile configured in this command.

```
[edit access profile]
user@host# set local_pf client test firewall-user password "$ABC123"
user@host# set local_pf client test1 client-group local-group1
user@host# set local_pf client test1 client-group local-group2
user@host# set local_pf client test1 firewall-user password "$BCD678"
user@host# set local_pf client test2 client-group local-group2
user@host# set local_pf client test2 firewall-user password "$DEF234"
user@host# set local_pf client test3 client-group local-group3
user@host# set local_pf client test3 firewall-user password "$DBC123"
user@host# set local_pf client test4 client-group local-group4
user@host# set local_pf client test4 firewall-user password "$FAB123"
```

2. Create an access profile to configure the RADIUS server.

```
[edit access profile]
user@host# set radius_pf authentication-order radius
user@host# set radius_pf radius-server 203.0.113.1 secret "$AFD123"
```

3. Create an access profile to configure SecurID as the server to be used for external authentication.

```
[edit access profile]
user@host# set securid_pf authentication-order securid
```

Step-by-Step Procedure

Configure different security policies that permit HTTP, HTTPS, and Telnet traffic between zones using pass-through (direct and web-redirect) and web authentication modes in a tenant system.

1. Configure policy p1 for pass-through authentication for Telnet traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 match application junos-
telnet
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p1 then permit firewall-
authentication pass-through access-profile local_pf
```

2. Configure policy p7 for pass-through authentication for HTTPS traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 match application junos-https
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 then permit firewall-
authentication pass-through access-profile local_pf
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p7 then permit firewall-
authentication pass-through ssl-termination-profile fwauthhttpspf
```

3. Configure policy p4 for pass through authentication using web-redirect for HTTP traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match source-address
ipv6_addr1
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 match application junos-http
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 then permit firewall-
```

```
authentication pass-through access-profile radius_pf
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p4 then permit firewall-
authentication pass-through web-redirect
```

4. Configure policy p3 for web authentication for HTTP traffic.

```
[edit tenants tn1 security policies]
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match source-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match destination-address any
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 match application junos-http
user@host# set from-zone tn1_trust to-zone tn1_untrust policy p3 then permit firewall-
authentication web-authentication
user@host# set policy-rematch
```

5. Configure zones and assign interfaces to each zone in a tenant system.

```
[edit tenants tn1 security zones]
user@host# set security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-traffic system-
services all
user@host# set security-zone tn1_trust interfaces xe-0/0/1.0 host-inbound-traffic protocols
all
user@host# set security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-traffic system-
services all
user@host# set security-zone tn1_untrust interfaces xe-0/0/2.0 host-inbound-traffic protocols
all
```

6. Define a success banner for Telnet sessions. Configure firewall authentication pass-through and web authentication banner for applications in a tenant system.

```
[edit tenants tn1 access firewall-authentication]
user@host# set pass-through default-profile local_pf
user@host# set pass-through telnet banner login ****tenant1_telnet_login_banner
user@host# set pass-through telnet banner success ****tenant1_telnet_success_banner
user@host# set pass-through telnet banner fail ****tenant1_telnet_fail_banner
user@host# set web-authentication default-profile securid_pf
user@host# set web-authentication banner success ****tenant1_webauth_success_banner
```

Results

From configuration mode, confirm your configuration by entering the `show system security-profile`, `show interfaces`, `show access`, `show tenants`, and `show services ssl termination` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show interfaces
xe-0/0/1 {
    unit 0 {
        family inet {
            address 192.0.2.0/24;
            address 192.0.2.254/24 {
                web-authentication {
                    http;
                    https;
                }
            }
        }
    }
}
xe-0/0/2 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}
```

```
user@host#show services ssl termination
profile fwauthhttpspf {
    server-certificate device;
}
```

```
user@host#show access
profile local_pf {
    client test {
        firewall-user {
            password "$ABC123"; ## SECRET-DATA
        }
```

```
    }
    client test1 {
        client-group [ local-group1 local-group2 ];
        firewall-user {
            password "$BCD678"; ## SECRET-DATA
        }
    }
    client test2 {
        client-group local-group2;
        firewall-user {
            password "$DEF234"; ## SECRET-DATA
        }
    }
    client test3 {
        client-group local-group3;
        firewall-user {
            password "$DBC123"; ## SECRET-DATA
        }
    }
    client test4 {
        client-group local-group4;
        firewall-user {
            password "$FAB123"; ## SECRET-DATA
        }
    }
    session-options {
        client-session-timeout 3;
    }
}
profile radius_pf {
    authentication-order radius;
    session-options {
        client-session-timeout 3;
    }
    radius-server {
        203.0.113.1 secret "$AFD123"; ## SECRET-DATA
    }
}
```

```
user@host#  show system security-profile
tn1_pf {
```

```
    policy {
        maximum 500;
        reserved 100;
    }
    zone {
        maximum 50;
        reserved 10;
    }
}
```

```
user@host#  show tenants
tn1 {
    routing-instances {
        vr1 {
            instance-type virtual-router;
            interface xe-0/0/1.0;
            interface xe-0/0/2.0;
        }
    }
    security-profile {
        tn1_pf;
    }
    security {
        policies {
            from-zone tn1_trust to-zone tn1_untrust {
                policy p2 {
                    match {
                        source-address any;
                        destination-address any;
                        application any;
                    }
                    then {
                        permit {
                            firewall-authentication {
                                pass-through {
                                    access-profile ldap_pf;
                                }
                            }
                        }
                    }
                }
```

```
            }
        }
        zones {
            security-zone tn1_trust {
                interfaces {
                    xe-0/0/1.0 {
                        host-inbound-traffic {
                            system-services {
                                all;
                            }
                            protocols {
                                all;
                            }
                        }
                    }
                }
            }
            security-zone tn1_untrust {
                interfaces {
                    xe-0/0/2.0 {
                        host-inbound-traffic {
                            system-services {
                                all;
                            }
                            protocols {
                                all;
                            }
                        }
                    }
                }
            }
        }
    }
    access {
        firewall-authentication {
            pass-through {
                default-profile local_pf;
                telnet {
                    banner {
                        login ****tenant1_telnet_login_banner;
                        success ****tenant1_telnet_success_banner;
                        fail ****tenant1_telnet_fail_banner;
                    }
```

```
                }
            }
            web-authentication {
                default-profile radius_pf;
                banner {
                    success ****tenant1_webauth_success_banner;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

- Verifying Firewall User Authentication and Monitoring Users and IP Addresses in the Authentication Table | **629**

Verifying Firewall User Authentication and Monitoring Users and IP Addresses in the Authentication Table

Purpose

The administrator for tenant system 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 tenant system. The administrator for the tenant system can use the same commands to view information for all tenant systems.

Action

From operational mode, enter the following show commands:

```
user@host> show security firewall-authentication history tenant tn1 identifier 10
Username: test
Source IP: 10.12.12.10Authentication state: Success
Authentication method: Pass-through using HTTP
```

```
Access start date: 2018-05-31
Access start time: 17:07:38
Duration of user access: 0:10:01
Lsys: root-logical-system
Tenant: tn1
Source zone: trust-tn1
Destination zone: untrust-tn1
Access profile: test
Bytes sent by this user: 380
Bytes received by this user: 0
user@host> show security firewall-authentication history tenant tn1
History of firewall authentication data:
  Authentications: 2
          Id Source Ip                         Date       Time     Duration   Status   User
           1 203.0.113.10                       2018-05-27 09:33:05 0:01:44    Success  test
           2 203.0.113.10                       2018-05-27 10:01:09 0:10:02    Success  test

user@host> show security firewall-authentication users tenant tn1
Firewall authentication data:
  Total users in table: 1
          Id Source Ip                         Src zone Dst zone Profile    Age Status
User
           2 203.0.113.10                         N/A      N/A      test         1 Success
test
```

Meaning

The output displays the authenticated firewall users and the firewall authentication history of the users for the tenant system

SEE ALSO

firewall-authentication

show security firewall-authentication history

show security firewall-authentication users

Understanding Integrated User Firewall Support in a Tenant System

IN THIS SECTION

Tenant system supports the user firewall authentication in shared and active mode.

Starting in Junos OS Release 19.1R1, user firewall authentication is supported on tenant systems using a shared model. In this model, the primary logical system shares the user firewall configuration and authentication entries with the tenant system. The primary logical system shares the authentication data with the tenant system, which is collected from the Local authentication, Active Directory (AD) authentication, firewall authenticationft, Juniper Identity Management Service (JIMS), and ClearPass authentication.

In the shared model, user firewall related configuration is configured under the primary logical system, such as authentication source, authentication source priority, authentication entries timeout, and IP query or individual query and so on. The user firewall provides user information service for an application on the SRX Series Firewall, such as policy and logging. Traffic from a tenant system queries the authentication tables from the primary logical system.

The authentication tables are managed by a primary logical system. The tenant systems share the authentication tables. Traffic from the primary logical system and the tenant systems query the same authentication table. Tenant systems enable the use of the source-identity in security policy.

For example, if the primary logical system is configured with **employee** and the tenant system is configured with the source-identity **manager**, then the reference group of this authentication entry includes **employee** and **manager**. This reference group contains the same authentication entries from primary logical system and tenant system.

Starting in Junos OS Release 19.3R1, support for user firewall authentication is enhanced by using a customized model through integrated JIMS with active mode. In this model, the tenant system extracts the authentication entries from the root level. The primary logical system is configured to the JIMS server based on the logical system and tenant system name. In active mode the SRX Series Firewall actively queries the authenticaton entries received from the JIMS server through HTTPs protocol. To reduce the data exchange, firewall filters are applied.

The user firewall uses the tenant system name as a diffrentiator and is consistent between the JIMS server and SRX Series Firewall. The JIMS server sends the diffrentiator which is included in the

authentication entry. The authentication entries are distributed into the root logical system, when the diffrentiator is set as default for the primary logical system.

The user firewall support In-service software upgrade (ISSU) for tenant systems, as user firewall changes the internal database table format from Junos OS Release 19.2R1 onwards. Prior to Junos OS Release 19.2R1, the ISSU is not supported for tenant systems.

Starting in Junos OS Release 20.2R1, logical systems and tenant systems support user firewall authentication with Unified Access Control (UAC).

Limitation of Using User Firewall Authentication in Tenant Systems

Using user firewall authentication on tenant systems has the following limitation:

- The IP addresses under different tenant systems must not overlap. If the address overlap, then the authentication entry is changed when different users log in under different tenant systems.

Limitation of using User Firewall Authentication in customized model on Tenant Systems

Using user firewall authentication in customized model on tenant systems has the following limitation:

- The JIMS server configurations to be configured under the root logical systems.
- The tenant system name should be consistent and unique between the JIMS server and the SRX Series Firewall.

SEE ALSO

show services user-identification authentication-table

Example: Configuring Integrated User Firewall Identification Management for a Tenant System

IN THIS SECTION

This example shows how to configure the SRX Series Firewall's advanced query feature for obtaining user identity information from the Juniper Identity Management Service (JIMS) and the security policy to match the source identity for a tenant system. In the primary logical system, user firewall is configured with JIMS, and then the primary logical system manages all of authentication entries coming from JIMS. In this example, the primary logical systems shares the authentication entries with the tenant systems.

Requirements

This example uses the following hardware and software components:

- SRX1500 devices operating in chassis clustering
- JIMS server
- Junos OS Release 19.1 R1

Overview

In this example, you can configure JIMS with HTTPs connection on port 443 and primary server with IPv4 address on the primary logical system, policy p1 with source-identity "group1" of dc0 domain on tenant system TN1, policy p1 with source-identity "group1" of dc0 domain on tenant system TN2, and send traffic from and through tenant system TN1 to tenant system TN2. You can view the authentication entries on primary logical system and tenant systems (TN1 and TN2) even after rebooting the primary node.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match
source-address any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match
destination-address any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match
application any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match
source-identity "example.com\group1"
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 then
permit
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2
match source-address any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2
match destination-address any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2
match application any
set tenants TN1 security policies from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2
then permit
set tenants TN1 security policies from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3
match source-address any
set tenants TN1 security policies from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3
match destination-address any
set tenants TN1 security policies from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3
match application any
set tenants TN1 security policies from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3
then permit
set tenants TN1 security policies policy-rematch
set tenants TN2 security policies from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1
match source-address any
set tenants TN2 security policies from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1
match destination-address any
set tenants TN2 security policies from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1
match application any
set tenants TN2 security policies from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1
match source-identity "example.com\group2"
set tenants TN2 security policies from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1
```

```
then permit
set tenants TN2 security policies policy-rematch
set services user-identification identity-management connection connect-method https
set services user-identification identity-management connection port 443
set services user-identification identity-management connection primary address 192.0.2.5
set services user-identification identity-management connection primary client-id otest
set services user-identification identity-management connection primary client-secret "$ABC123"
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match source-
address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
destination-address any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 match
application any
set security policies from-zone root_trust to-zone root_trust policy root_policy1 then permit
set security policies policy-rematch
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic system-
services all
set security zones security-zone root_trust interfaces reth1.0 host-inbound-traffic protocols all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic system-
services all
set security zones security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic protocols
all
set firewall family inet filter impair-ldap term allow_all then accept
```

Configuring user firewall identification management

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 user firewall identification management:

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

```
user@host> configure
user@host#
```

2. Create tenant systems.

```
[edit tenants]
user@host#set TN1
user@host#set TN2
```

3. Configure a security policy TN1_policy1 with source-identity group1 on the tenant system TN1 that permits traffic from TN1_trust to TN1_trust.

```
[edit security policies]
user@host#set from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match source-address
any
user@host#set from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match destination-
address any
user@host#set from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match application any
user@host#set from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 match source-
identity "example.com\group1"
user@host#set from-zone TN1_trust to-zone TN1_trust policy TN1_policy1 then permit
```

4. Configure a security policy TN1_policy2 that permits traffic from TN1_trust to TN1_untrust.

```
[edit security policies]
user@host#set from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2 match source-
address any
user@host#set from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2 match destination-
address any
user@host#set from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2 match application
any
user@host#set from-zone TN1_trust to-zone TN1_untrust policy TN1_policy2 then permit
```

5. Configure a security policy TN1_policy3 that permits traffic from TN1_untrust to TN1_trust.

```
[edit security policies]
user@host#set from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3 match source-
address any
user@host#set from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3 match destination-
address any
user@host#set from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3 match application
any
```

```
user@host#set from-zone TN1_untrust to-zone TN1_trust policy TN1_policy3 then permit
user@host#set policy-rematch
```

6. Configure security zone and assign interfaces to each zone.

```
[edit security zones]
user@host#set security-zone TN1_trust interfaces reth2.0 host-inbound-traffic system-
services all
user@host#set security-zone TN1_trust interfaces reth2.0 host-inbound-traffic protocols all
user@host#set security-zone TN1_trust interfaces lt-0/0/0.11 host-inbound-traffic system-
services all
user@host#set security-zone TN1_trust interfaces lt-0/0/0.11 host-inbound-traffic protocols
all
user@host#set security-zone TN1_untrust interfaces reth3.0 host-inbound-traffic system-
services all
user@host#set security-zone TN1_untrust interfaces reth3.0 host-inbound-traffic protocols
all
```

7. Configure a security policy TN2_policy1 with source-identity group1 that permits traffic from TN2_untrust to TN2_untrust on TN2.

```
[edit security policies]
user@host#set from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1 match source-
address any
user@host#set from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1 match
destination-address any
user@host#set from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1 match
application any
user@host#set from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1 match source-
identity "example.com\group2"
user@host#set from-zone TN2_untrust to-zone TN2_untrust policy TN2_policy1 then permit
user@host#set policy-rematch
```

8. Configure security zones and assign interfaces to each zone on TN2.

```
[edit security zones]
user@host#set security-zone TN2_untrust interfaces reth4.0 host-inbound-traffic system-
services all
user@host#set security-zone TN2_untrust interfaces reth4.0 host-inbound-traffic protocols
all
```

```
user@host#set security-zone TN2_untrust interfaces lt-0/0/0.21 host-inbound-traffic system-
services all
user@host#set security-zone TN2_untrust interfaces lt-0/0/0.21 host-inbound-traffic
protocols all
```

9. Configure JIMS as the authentication source for advanced query requests with the primary address. The SRX Series Firewall requires this information to contact the server.

```
[edit services user-identification identity-management]
user@host#set connection port 443
user@host#set connection connect-method https
user@host#set connection primary address 192.0.2.5
user@host#set connection primary client-id otest
user@host#set connection primary client-secret test
user@host#set authentication-entry-timeout 0
```

10. Configure security policies and zones on the primary logical system.

```
[edit security policies]
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match source-
address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match destination-
address any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 match application
any
user@host#set from-zone root_trust to-zone root_trust policy root_policy1 then permit
user@host#set policy-rematch
```

11. Configure security zones and assign interfaces to each zone on primary logical system.

```
[edit security zones]
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic system-
services all
user@host#set security-zone root_trust interfaces reth1.0 host-inbound-traffic protocols all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic system-
services all
user@host#set security-zone root_trust interfaces lt-0/0/0.1 host-inbound-traffic protocols
all
user@host#set firewall family inet filter impair-ldap term allow_all then accept
```

Results

From configuration mode, confirm your configuration by entering the `show services user-identification identity-management` `show chassis cluster` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show services user-identification identity-management
connection {
    connect-method https;
    port 443;
    primary {
        address 192.0.2.5;
        client-id otest;
        client-secret "$ABC123"; ## SECRET-DATA
    }
}
```

```
user@host# show chassis cluster
reth-count 5;
    control-ports {
    fpc 3 port 0;
    fpc 9 port 0;
}
redundancy-group 0 {
    node 0 priority 200;
    node 1 priority 1;
}
redundancy-group 1 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 2 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 3 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 4 {
    node 0 priority 100;
```

```
    node 1 priority 1;
}
```

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

Verification

IN THIS SECTION

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

Verifying chassis cluster status and authentication entries

Purpose

To verify authentication entries in a tenant system.

Action

To verify the configuration is working properly, enter the `show services user-identification authentication-table authentication-source identity-management tenant TN1` command.

```
user@host> show services user-identification authentication-table authentication-source identity-
management tenant TN1
node0:
--------------------------------------------------------------------------
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP       Username       groups(Ref by policy)          state
2001:db8:aaaa:  N/A                                           Valid
2001:db8:aaaa:  administrator                                 Valid
203.0.113.50    administrator                                 Valid
node1:
--------------------------------------------------------------------------
```

```
Logical System: root-logical-system
Domain: ad2012.jims.com
Total entries: 3
Source IP       Username       groups(Ref by policy)         state
2001:db8:aaaa:  N/A                                          Valid
2001:db8:aaaa:  administrator                                Valid
203.0.113.50    administrator                                Valid
```

Meaning

The output displays the authentication entries that are shared from the primary logical system to the tenant system.

Verifying chassis cluster status

Purpose

Verify chassis cluster status after rebooting the primary node.

Action

To verify the configuration is working properly, enter the `show chassis cluster status` command.

```
user@host> show chassis cluster status
Monitor Failure codes:
CS  Cold Sync monitoring        FL  Fabric Connection monitoring
GR  GRES monitoring             HW  Hardware monitoring
IF  Interface monitoring        IP  IP monitoring
LB  Loopback monitoring         MB  Mbuf monitoring
NH  Nexthop monitoring          NP  NPC monitoring
SP  SPU monitoring              SM  Schedule monitoring
CF  Config Sync monitoring      RE  Relinquish monitoring
Cluster ID: 6
Node   Priority Status               Preempt Manual   Monitor-failures
Redundancy group: 0 , Failover count: 0
node0  200      hold                 no      no       None
node1  1        secondary            no      no       None
Redundancy group: 1 , Failover count: 0
node0  0        hold                 no      no       CS
node1  1        secondary            no      no       None
Redundancy group: 2 , Failover count: 0
```

```
node0  0        hold                no      no      CS
node1  1        secondary           no      no      None
Redundancy group: 3 , Failover count: 0
node0  0        hold                no      no      CS
node1  1        secondary           no      no      None
Redundancy group: 4 , Failover count: 0
node0  0        hold                no      no      CS
node1  1        secondary           no      no      None
```

Meaning

The output displays user identification management session existing on TN1 and TN2 after rebooting the primary node.

SEE ALSO

show services user-identification authentication-table

Example: Configure Integrated User Firewall in Customized Model for Tenant System

IN THIS SECTION

This example shows how to configure the integrated user firewall by using a customized model through the Juniper Identity Management Service (JIMS) server with active mode for a tenant system. The primary logical systems does not share the authentication entries with the tenant systems. The SRX Series Firewall queries the authentication entries received from the JIMS server through HTTPs protocol in active mode.

In this example following configurations are performed:

- Active JIMS Server Configuration
- Tenant System IP Query Configuration
- Tenant System Authentication Entry Configuration
- Tenant System Security Policy Configuration

Requirements

This example uses the following hardware and software components:

- JIMS server version 2.0
- Junos OS Release 19.3R1

Before you begin, be sure you have following information:

- The IP address of the JIMS server.
- The port number on the JIMS server for receiving HTTPs requests.
- The client ID from the JIMS server for active query server.
- The client secret from the JIMS server for active query server.

Overview

In this example, you can configure JIMS with HTTPs connection on port 443 and primary server with IPv4 address on the primary logical system, policy p2 with source-identity `group1` on tenant system `TSYS1`.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set services user-identification logical-domain-identity-management active query-server jims1
connection connect-method https
set services user-identification logical-domain-identity-management active query-server jims1
connection port 443
set services user-identification logical-domain-identity-management active query-server jims1
connection primary address 192.0.2.5
set services user-identification logical-domain-identity-management active query-server jims1
connection primary client-id otest
set services user-identification logical-domain-identity-management active query-server jims1
connection primary client-secret "$ABC123"
set tenants TSYS1 services user-identification logical-domain-identity-management active ip-
query query-delay-time 30
set tenants TSYS1 services user-identification logical-domain-identity-management active invalid-
authentication-entry-timeout 1
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match source-
address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match destination-
address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match application
any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match source-
identity "example.com\group1"
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 then permit
```

Configuring Integrated User Firewall in Customized Model:

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 Integrated User Firewall in Customized Model:

1. Configure JIMS as the authentication source for advanced query requests with the primary address. The SRX Series Firewall requires this information to contact the server.

```
user@host# set services user-identification logical-domain-identity-management active query-server jims1 connection connect-method https
user@host# set services user-identification logical-domain-identity-management active query-server jims1 connection port 443
user@host# set services user-identification logical-domain-identity-management active query-server jims1 connection primary address 192.0.2.5
user@host# set services user-identification logical-domain-identity-management active query-server jims1 connection primary client-id otest
user@host# set services user-identification logical-domain-identity-management active query-server jims1 connection primary client-secret "$ABC123"
```

2. Configure the IP query delay time for TSYS1.

```
user@host# set tenants TSYS1 services user-identification logical-domain-identity-management active ip-query query-delay-time 30
```

3. Configure the authentication entry attributes for TSYS1.

```
user@host# set tenants TSYS1 services user-identification logical-domain-identity-management active invalid-authentication-entry-timeout 1
```

4. Configure the security policy p2 that permits traffic from-zone untrust to-zone trust for TSYS1.

```
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match source-address any
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match destination-address any
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match application any
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match source-identity "example.com\group1"
user@host#set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 then permit
```

Results

From configuration mode, confirm your configuration by entering the `show services user-identification logical-domain-identity-management` and `show tenants TSYS1` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show services user-identification logical-domain-identity-management
active {
    query-server jims1 {
        connection {
            connect-method https;
            port 443;
            primary {
                address 10.1.1.1;
                client-id otest;
                client-secret "$ABC123"; ## SECRET-DATA
            }
        }
    }
}
```

```
user@host# show tenants TSYS1
security {
    policies {
        from-zone untrust to-zone trust {
            policy p2 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                    source-identity "example.com\group1";
                }
                then {
                    permit;
                }
            }
        }
    }
}
services {
    user-identification {
```

```
        logical-domain-identity-management {
            active {
                invalid-authentication-entry-timeout 1;
                ip-query {
                    query-delay-time 30;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the User Identification Identity Management status

Purpose

Verify the user identification status for identity-management as the authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification logical-domain-identity-management status` command.

```
user@host>show services user-identification logical-domain-identity-management status
node0:
--------------------------------------------------------------------------
      Query server name                :jims1
```

```
      Primary server :
     Address                      : 10.1.1.1
     Port                         : 443
     Connection method            : HTTPS
     Connection status            : Online
     Last received status message : OK (200)
     Access token                 : isdHIbl8BXwxFftMRubGVsELRukYXtW3rtKmHiL
     Token expire time            : 2017-11-27 23:45:22
     Secondary server :
     Address                      : Not configured
```

Meaning

The output displays the statistical data about the advanced user query function batch queries and IP queries, or show status on the Juniper Identity Management Service servers.

Verifying the User Identification Identity Management status counters

Purpose

Verify the user identification counters for identity-management as the authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification logical-domain-identity-management counters` command.

```
user@host>show services user-identification logical-domain-identity-management counters
node0:
      --------------------------------------------------------------------------
   Query server name                      :jims1
    Primary server :
     Address                           : 10.208.137.208
     Batch query sent number           : 65381
     Batch query total response number : 64930
     Batch query error response number : 38
     Batch query last response time    : 2018-08-14 15:10:52
     IP query sent number              : 10
     IP query total response number    : 10
     IP query error response number    : 0
     IP query last response time       : 2018-08-13 12:41:56
```

```
  Secondary server :
 Address                          : Not configured
```

Meaning

The output displays the statistical data about the advanced user query function batch queries and IP queries, or show counters on the Juniper Identity Management Service servers.

Verifying the User Identification Authentication Table

Purpose

Verify the user identity information authentication table entries for the specified authentication source.

Action

To verify the configuration is working properly, enter the `show services user-identification authentication-table authentication-source all tenant TSYS1` command.

```
user@host>show services user-identification authentication-table authentication-source all tenant TSYS1
node0:
      --------------------------------------------------------------------------
   Tenant System: TSYS1
Domain: ad03.net
Total entries: 4
Source IP       Username       groups(Ref by policy)          state
10.12.0.2        administrator  posture-healthy                Valid
10.12.0.15       administrator  posture-healthy                Valid
2001:db8:3000::5         N/A            posture-healthy                Valid
fe80::342c:302b N/A            posture-healthy                Valid
```

Meaning

The output displays the entire content of the specified authentication source's authentication table, or a specific domain, group, or user based on the user name. Display the identity information for a user based on the IP address of the user's device.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.3R1	Starting in Junos OS Release 19.3R1, support for user firewall authentication is enhanced by using a customized model through integrated JIMS with active mode.
19.1R1	Starting in Junos OS Release 19.1R1, user firewall authentication is supported on tenant systems using a shared model. In this model, the primary logical system shares the user firewall configuration and authentication entries with the tenant system. The primary logical system shares the authentication data with the tenant system, which is collected from the Local authentication, Active Directory (AD) authentication, firewall authenticationft, Juniper Identity Management Service (JIMS), and ClearPass authentication.

Security Policies for Tenant Systems

IN THIS SECTION

Security policies can be configured with tenant systems. For more information see the following topics:

Understanding Security Policies for Tenant Systems

IN THIS SECTION

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. Through the creation of security policies, the administrator for the tenant system can control the traffic flow from zone to zone by defining the kinds of traffic permitted to pass from sources to destinations. From the perspective of the security policies, traffic enters one security zone and exits through another security zone. By default, the tenant system denies all traffic in all directions, including intra-zone and inter-zone directions.

Starting in Junos OS Release 18.3R1, the security policies feature supported on logical systems is now extended to tenant systems.

Security policies can be configured in the tenant systems. Tenant security policies are configured the same way as logical system security policies and firewall-wide security policies. Any security policies, policy rules, address books, applications and application sets, and schedulers created within a tenant system are only applicable to that tenant system. Only predefined applications and application sets, such as `junos-ftp`, are shared between the tenant systems.

The administrator for the tenant system can configure and view all attributes for security policies in a tenant system.

Starting in Junos OS Release 18.4R1, the tenant system administrator can create dynamic address within a tenant system. A dynamic address entry contains IP addresses and prefixes extracted from external sources. The security policies use the dynamic address in the source-address field or destination-address field. You can view the dynamic-address information including the name, feeds, and properties for tenant systems by using the command `show security dynamic-address`.

A dynamic address entry (DAE) is a group of IP addresses that can be entered manually or imported from external sources within tenant systems. The DAE feature allows feed-based IP objects to be used in security policies to either deny or allow traffic based on either source or destination IP criteria.

NOTE: The maximum number of DAE for a given tenant system equals the system-wide scaling number. Furthermore, the sum of DAE for all the tenant systems must be less than or equal to the system-wide scaling number for DAE. If one tenant system uses maximum number of IP entries, other tenant system will fail to get IP entries into their DAE.

Starting in Junos 18.4R1, the `set security dynamic-address feed-server` command can be configured under the tenant systems.

Application Timeouts

The application timeout value set for an application determines the session timeout. Application timeout behavior is the same for a tenant system as it is at the root level. Although the administrators of the tenant system can use predefined applications in security policies, the administrators cannot modify the

timeout value for these predefined applications. Application timeout values are stored in the application entry database and in the corresponding tenant system TCP and UDP port-based timeout tables.

Security Policy Allocation

The primary administrator creates a security profile to allocate the maximum number of policies that can be configured for each tenant system. The administrator of the tenant system is then restricted by the security profile to create no more than the number of policies described in the security profile. The administrator of the tenant system use the `show system security-profile policy` command to view the number of security policies allocated to the tenant system.

```
user@host> show system security-profile policy
```

```
logical-system tenant name   security profile name       usage    reserved     maximum

root-logical-system          Default-Profile                1           0       16000
```

Example: Configuring Security Policies in the Tenant System

IN THIS SECTION

This example shows how to configure the security policies for the tenant system.

Requirements

Before you begin the configuration:

- Configure zones. See *Example: Configuring Security Zones in the Tenant System*.

- Use the `show system security-profiles policy` command to see the security policy resources allocated to the tenant system.

Overview

In this example, you can configure a security policy for the tenant system. The administrator for the tenant system user can use `[edit tenants tenant-name security policies]` hierarchy level to configure the security policies. This example configures the security policies described in Table 37 on page 653.

Table 37: Security Policies Parameters

Feature	Configuration Parameters
Policy 1	Permit the following traffic: • Policy name: p1 • Tenant name: TSYS1 • From zone: trust • To zone: untrust • Source address: any • Destination address: any • Application: any
Policy 2	Permit the following traffic: • Policy name: p1 • Tenant name: TSYS1 • From zone: untrust • To zone: trust • Source address: any • Destination address: any • Application: any

Configuration

IN THIS SECTION

- Procedure | 654

Procedure

CLI Quick Configuration

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

```
set tenants TSYS1 security policies from-zone trust to-zone untrust policy p1 match source-
address any
set tenants TSYS1 security policies from-zone trust to-zone untrust policy p1 match destination-
address any
set tenants TSYS1 security policies from-zone trust to-zone untrust policy p1 match application
any
set tenants TSYS1 security policies from-zone trust to-zone untrust policy p1 then permit
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match source-
address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match destination-
address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 match application
any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy p2 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 the security policies in the tenant system:

1. Log in to the tenant system and define the tenant system name as TSYS1.

```
[edit]
user@host# set tenants TSYS1
```

2. Create a security policy as p1 that permits traffic from zone trust to zone untrust and configure the match condition.

```
[edit tenants TSYS1 security policies from-zone trust to-zone untrust]
user@host# set policy p1 match source-address any
user@host# set policy p1 match destination-address any
user@host# set policy p1 match application any
user@host# set policy p1 then permit
```

3. Create a security policy as p2 that permits traffic from zone untrust to zone trust and configure the match condition.

```
[edit tenants TSYS1 security policies from-zone untrust to-zone trust]
user@host# set policy p2 match source-address any
user@host# set policy p2 match destination-address any
user@host# set policy p2 match application any
user@host# set policy p2 then permit
```

Results

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

```
user@host# show tenants TSYS1 security policies
from-zone trust to-zone untrust {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
```

```
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify the information about security policies.

Action

To verify the configuration is working properly, enter the `show security policies detail tenant TSYS1` command from operational mode.

```
user@host> show security policies detail tenant TSYS1
```

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: any
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input  bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Output bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Input  packets   :                   0                   0 pps
Initial direction:                   0                   0 bps
```

```
Reply direction   :                0                    0 bps
Output packets    :                0                    0 pps
Initial direction:                 0                    0 bps
Reply direction   :                0                    0 bps
Session rate      :                0                    0 sps
Active sessions   :                0
Session deletions:                 0
Policy lookups    :                0
```

Meaning

The output displays the information about the security policies configured on the tenant system.

Configuring Dynamic Address for Tenant Systems

A dynamic address entry in the tenant system provides dynamic IP address information to security policies. To use dynamic address, you must specify basic information of dynamic address including their names, feeds and properties for a tenant system.

- Read the "Example: Configuring Security Policies in the Tenant System" on page 652 to understand how and where this procedure fits in the overall tenant support for security policy.

To configure the dynamic address in IPv4 networks within a tenant system:

1. Define the tenant system name as TSYS1.

```
[edit]
user@host# set tenants TSYS1
```

2. Create dynamic address within a tenant system.

```
[edit tenants TSYS1]
user@host# set security dynamic-address address-name Ipv4 profile category IPFilter feed fd1
```

3. Confirm your configuration by entering the `show tenants TSYS1 security dynamic-address` command.

```
[edit]
user@host# show tenants TSYS1 security dynamic-address
address-name Ipv4 {
```

```
    profile {
        category GeoIP;
        category IPFilter {
            feed fd1;
            }
        }
    }
}
```

- To configure the security policies in the tenant system:

  1. Define the tenant system name as TSYS1.

     ```
     [edit]
     user@host# set tenants TSYS1
     ```

  2. Create a security policy as p1 that permits traffic from zone trust to zone untrust and configure the match condition.

     ```
     [edit tenants TSYS1 security policies from-zone trust to-zone untrust]
     user@host# set policy p1 match source-address any
     user@host# set policy p1 match destination-address any
     user@host# set policy p1 match application any
     user@host# set policy p1 then permit
     ```

  3. Confirm your configuration by entering the `show tenants tenant-name security policies` command

     ```
     [edit]
     user@host# show tenants TSYS1 security policies
     from-zone trust to-zone untrust {
         policy p1 {
             match {
                 source-address any;
                 destination-address any;
                 application any;
             }
             then {
                 permit;
             }
     ```

```
    }
}
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the security policies feature supported on logical systems is now extended to tenant systems.

RELATED DOCUMENTATION

- Tenant Systems Overview | 525

Screen Options for Tenant Systems

IN THIS SECTION

Screen options for Tenant Systems on SRX Series Firewalls prevent attacks as , such as IP address sweeps, port scans, denial of service (DOS) attacks, ICMP, UDP, and SYN floods as same as Logical Systems. For more information, see the following topics:

Understanding Tenant System Screen Options

Using screen options, the device secures a zone by inspecting, and then allowing or denying all connection attempts that require crossing an interface bound to that zone. Junos OS applies the firewall policies, which can contain the content filtering and the IDP components to the traffic that passes the screen filters. All screen options that are available on the device are also available in each tenant system.

Starting in Junos OS Release 18.3R1, the screen options that are supported for logical systems are extended to tenant systems.

SEE ALSO

Understanding Screens Options on SRX Series Devices

Example: Configuring Screen Options for a Tenant System

IN THIS SECTION

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

Requirements

Before you begin:

- Understand the tenant system configuration process. See "Tenant System Configuration Overview" on page 533 to understand how this task fits into the overall configuration process.
- Configure the zones for the tenant system. See "Security Zones for Tenant Systems" on page 568to understand how to configure the zones for the tenant systems.

Overview

Using screen options, the security device can protect against the different internal and external attacks for security zones. You can limit the number of concurrent sessions to the same destination IP address in a tenant 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.

Configuration

IN THIS SECTION

- Procedure | 662

Procedure

CLI Quick Configuration

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

```
set tenants TN1 security screen ids-option jscreen limit-session destination-ip-based 80
set tenants TN1 security screen ids-option jscreen icmp ip-sweep threshold 1000
set tenants TN1 security screen ids-option jscreen icmp fragment
set tenants TN1 security screen ids-option jscreen icmp large
set tenants TN1 security screen ids-option jscreen icmp flood threshold 200
set tenants TN1 security screen ids-option jscreen icmp ping-death
set tenants TN1 security screen ids-option jscreen ip bad-option
set tenants TN1 security screen ids-option jscreen ip stream-option
set tenants TN1 security screen ids-option jscreen ip spoofing
set tenants TN1 security screen ids-option jscreen ip strict-source-route-option
set tenants TN1 security screen ids-option jscreen ip unknown-protocol
set tenants TN1 security screen ids-option jscreen ip tear-drop
set tenants TN1 security screen ids-option jscreen tcp syn-fin
set tenants TN1 security screen ids-option jscreen tcp tcp-no-flag
set tenants TN1 security screen ids-option jscreen tcp syn-frag
set tenants TN1 security screen ids-option jscreen tcp port-scan threshold 1000
set tenants TN1 security screen ids-option jscreen tcp syn-ack-ack-proxy threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood alarm-threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood attack-threshold 500
set tenants TN1 security screen ids-option jscreen tcp syn-flood source-threshold 50
set tenants TN1 security screen ids-option jscreen tcp syn-flood destination-threshold 1000
set tenants TN1 security screen ids-option jscreen tcp syn-flood timeout 10
set tenants TN1 security screen ids-option jscreen tcp land
set tenants TN1 security screen ids-option jscreen tcp winnuke
set tenants TN1 security screen ids-option jscreen tcp tcp-sweep threshold 1000
```

```
set tenants TN1 security screen ids-option jscreen udp flood threshold 500
set tenants TN1 security screen ids-option jscreen udp udp-sweep threshold 1000
set tenants TN1 security zones security-zone untrust screen jscreen
```

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 tenant system:

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

```
user@host:TN1#> configure
user@host:TN1#
```

2. Define the tenant system name as TN1 and configure a screen option for a destination-based session limit.

```
[edit tenants TN1]
user@host:TN1# set security screen ids-option jscreen limit-session destination-ip-based 80
```

3. Configure the ICMP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set icmp ip-sweep threshold 1000
user@host:TN1# set icmp fragment
user@host:TN1# set icmp large
user@host:TN1# set icmp flood threshold 200
user@host:TN1# set icmp ping-death
```

4. Configure the IP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set ip bad-option
user@host:TN1# set ip stream-option
user@host:TN1# set ip spoofing
user@host:TN1# set ip strict-source-route-option
```

```
user@host:TN1# set ip unknown-protocol
user@host:TN1# set ip tear-drop
```

5. Configure the TCP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set tcp syn-fin
user@host:TN1# set tcp tcp-no-flag
user@host:TN1# set tcp syn-frag
user@host:TN1# set tcp port-scan threshold 1000
user@host:TN1# set tcp syn-ack-ack-proxy threshold 500
user@host:TN1# set tcp syn-flood alarm-threshold 500
user@host:TN1# set tcp syn-flood attack-threshold 500
user@host:TN1# set tcp syn-flood source-threshold 50
user@host:TN1# set tcp syn-flood destination-threshold 1000
user@host:TN1# set tcp syn-flood timeout 10
user@host:TN1# set tcp land
user@host:TN1# set tcp winnuke
user@host:TN1# set tcp tcp-sweep threshold 1000
```

6. Configure the UDP screening options.

```
[edit tenants TN1 security screen ids-option jscreen]
user@host:TN1# set udp flood threshold 500
user@host:TN1# set udp udp-sweep threshold 1000
```

7. Attach the IDS profile to the zone.

```
[edit tenants TN1]
user@host:TN1# set security zones security-zone untrust screen jscreen
```

Results

From configuration mode, confirm your configuration by entering the `show tenants TN1 security screen` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TN1 security screen
ids-option jscreen {
    limit-session {
        destination-ip-based 80;
    }
}
ids-option jscreen {
    icmp {
        ip-sweep threshold 1000;
        fragment;
        large;
        flood threshold 200;
        ping-death;
    }
    ip {
        bad-option;
        stream-option;
        spoofing;
        strict-source-route-option;
        unknown-protocol;
        tear-drop;
    }
    tcp {
        syn-fin;
        tcp-no-flag;
        syn-frag;
        port-scan threshold 1000;
        syn-ack-ack-proxy threshold 500;
        syn-flood {
            alarm-threshold 500;
            destination-threshold 1000;
            timeout 10;
        }
        land;
        winnuke;
        tcp-sweep threshold 1000;
```

```
    }
    udp {
        flood {
            threshold 500;
        }
        udp-sweep threshold 1000;
    }
}
```

Verification

IN THIS SECTION

- Verifying security screen status | **666**

To confirm that the configuration is working properly, perform the below task:

Verifying security screen status

Purpose

Verify that the IDS profile for multiple screening options is configured properly:

Action

To verify the configuration is working properly, enter the `show security screen ids-option jscreen tenant TN1` and `show security zone tenant TN1`command from operational mode.

```
user@host> show security screen ids-option jscreen tenant TN1

  Screen object status:

  Name                                    Value
  ICMP flood threshold                    200
  UDP flood threshold                     500
  TCP winnuke                             enabled
  TCP port scan threshold                 1000
  ICMP address sweep threshold            1000
```

```
  TCP sweep threshold                     1000
  UDP sweep threshold                     1000
  IP tear drop                            enabled
  TCP SYN flood attack threshold          500
  TCP SYN flood alarm threshold           500
  TCP SYN flood source threshold          50
  TCP SYN flood destination threshold     1000
  TCP SYN flood timeout                   10
  IP spoofing                             enabled
  ICMP ping of death                      enabled
  TCP land attack                         enabled
  TCP SYN fragment                        enabled
  TCP no flag                             enabled
  IP unknown protocol                     enabled
  IP bad options                          enabled
  IP strict source route option           enabled
  IP stream option                        enabled
  ICMP fragmentation                      enabled
  ICMP large packet                       enabled
  TCP SYN FIN                             enabled
  TCP SYN-ACK-ACK proxy threshold         500
```

```
user@host> show security zone tenant TN1

Security zone: untrust
Send reset for non-SYN session TCP packets: Off
Policy configurable: Yes
Screen: jscreen
Interfaces bound: 0
Interfaces:
```

Meaning

The output displays the screen status in the tenant system.

SEE ALSO

Understanding Tenant System Screen Options | 660

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the screen options that are supported for logical systems are extended to tenant systems.

RELATED DOCUMENTATION

Example: Creating Tenant Systems, Tenant System Administrators, and an Interconnect VPLS Switch

NAT for Tenant Systems

IN THIS SECTION

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. For more information, see the following topics:

Understanding Network Address Translation for Tenant systems

Starting in Junos OS Release 18.3R1, the network address translation including source NAT, destination NAT, and static NAT supported on logical systems is supported on tenant systems.

A tenant system has an administrator (tenant administrator) who can configure source NAT, destination NAT, and static NAT for the tenant systems. The tenant administrator can view the details of the source NAT, destination NAT, and static NAT of the tenant system. The primary administrator can view the statistics or information of the source NAT, destination NAT, and static NAT for any tenant systems.

For the tenant system, the primary administrator can configure the maximum and reserved numbers for the following NAT resources:

- Source NAT pools and destination NAT pools
- IP addresses in the source NAT pools with and without port address translation
- Rules for source, destination, and static NAT
- Prefix list for rule matching
- NAT cone binding
- IP addresses that support port overloading

The reserved numbers allocated guarantees that the specified resource amount is constantly available to the tenant systems. The administrator for tenant systems can use the `show system security-profile` command with a NAT option to view the NAT resources allocated to the tenant system.

SEE ALSO

Understanding Network Address Translation for Tenant systems | **668**

Introduction to NAT

Example: Configuring Network Address Translation for the Tenant Systems

IN THIS SECTION

This example shows how to configure source NAT, destination NAT and static NAT for a given tenant systems.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall with Junos OS Release 18.3R1 or later. This configuration example is tested for Junos OS Release 18.3R1.
- Create tenant system. See : Example: Creating Tenant Systems, Tenant System Administrators, and an Interconnect VPLS Switch
- Configure network interfaces. See : "Configuring a Routing Instance for a Tenant System" on page 535.

Overview

In this example, first you configure the trust security zone for the private address space and then you configure the untrust security zone for the public address space.

Devices in the untrust zone access a specific host in the trust zone, with the destination IP address 203.0.113.200/24. This example configures the NAT described in Table 1: Tenant System NAT Configuration.

Table 38: Tenant System NAT Configuration

Feature	Name	Configuration Parameters
Static, source and destination NAT rule set	r1	• Rule r1 to match packets from untrust zone with destination address. • Destination IP address in matching packets is translated.
Source pool	pat	Address 192.0.2.1 to 192.0.2.24.
Destination pool	h1	Address 192.168.1.200.
Proxy ARP	arp	Address 192.0.2.1 to 192.0.2.24.
NAT interfaces for traffic direction.		ge-0/0/0 and ge-0/0/1.

Configuration

IN THIS SECTION

- Procedure | 671

Procedure

CLI Quick Configuration

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

```
set tenants tn1 security nat source pool pat address 192.0.2.1 to 192.0.2.24
set tenants tn1 security nat source rule-set from_intf from interface ge-0/0/0.0
set tenants tn1 security nat source rule-set from_intf to interface ge-0/0/1.0
set tenants tn1 security nat source rule-set from_intf rule r1 match source-address 192.0.2.0/24
set tenants tn1 security nat source rule-set from_intf rule r1 match destination-address
203.0.113.200/24
set tenants tn1 security nat source rule-set from_intf rule r1 then source-nat pool pat
set tenants tn1 security nat static rule-set from_zone from zone trust
set tenants tn1 security nat static rule-set from_zone rule r1 match source-address 192.0.2.0/24
set tenants tn1 security nat static rule-set from_zone rule r1 match destination-address
203.0.113.203/24
set tenants tn1 security nat static rule-set from_zone rule r1 then static-nat prefix
192.168.1.203/24
set tenants tn1 security nat destination pool h1 address 192.168.1.200
set tenants tn1 security nat destination rule-set from_zone from zone trust
set tenants tn1 security nat destination rule-set from_zone rule r1 match source-address
192.0.2.0/24
set tenants tn1 security nat destination rule-set from_zone rule r1 match destination-address
203.0.113.202/24
set tenants tn1 security nat destination rule-set from_zone rule r1 then destination-nat pool h1
set tenants tn1 security nat proxy-arp interface ge-0/0/1.0 address 192.0.2.1 to 192.0.2.24
```

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 configure NAT in the tenant system:

1. Create a security NAT source pool and rule set for the tenant system.

```
[edit tenant tn1 security nat source]
user@host# set tenants tn1 security nat source pool pat address 192.0.2.1 to 192.0.2.24
user@host# set tenants tn1 security nat source rule-set from_intf from interface ge-0/0/0.0
user@host# set tenants tn1 security nat source rule-set from_intf to interface ge-0/0/1.0
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 match source-
address 192.0.2.0/24
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 match destination-
address 203.0.113.200/24
user@host# set tenants tn1 security nat source rule-set from_intf rule r1 then source-nat
pool pat
```

2. Create a security NAT static rule set for the tenant system.

```
[edit tenants tn1 security nat static]
user@host# set tenants tn1 security nat static rule-set from_zone from zone trust
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 match source-
address 192.0.2.0/24
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 match destination-
address 203.0.113.203/24
user@host# set tenants tn1 security nat static rule-set from_zone rule r1 then static-nat
prefix 192.168.1.203/24
```

3. Create a security NAT destination pool and rule set for the tenant system.

```
[edit tenants tn1 security nat destination]
user@host# set tenants tn1 security nat destination pool h1 address 192.168.1.200
user@host# set tenants tn1 security nat destination rule-set from_zone from zone trust
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 match source-
address 192.0.2.0/24
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 match
destination-address 203.0.113.202/24
```

```
user@host# set tenants tn1 security nat destination rule-set from_zone rule r1 then
destination-nat pool h1
```

4. Configure proxy Address Resolution Protocol (ARP).

```
[edit tenant tn1 security nat]
user@host# set tenants tn1 security nat proxy-arp interface ge-0/0/1.0 address 192.0.2.1 to
192.0.2.24
```

Results

From configuration mode, confirm your configuration by entering the `show tenants tn1 security nat` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
source {
    pool pat {
        address {
            192.0.2.1 to 192.0.2.24;
        }
    }
    rule-set from_intf {
        from interface ge-0/0/0.0;
        to interface ge-0/0/1.0;
        rule r1 {
            match {
                source-address 192.168.1.0/24;
                destination-address [203.0.113.200/24 ];
            }
            then {
                source-nat {
                    pool {
                        pat;
                    }
                }
            }
        }
    }
}
destination {
```

```
    pool h1 {
        address 192.168.1.200;
    }
    rule-set from_zone {
        from zone untrust;
        rule r1 {
            match {
                source-address 192.0.2.0/24;
                destination-address 203.0.113.202/24;
            }
            then {
                destination-nat {
                    pool {
                        h1;
                    }
                }
            }
        }
    }
}
static {
    rule-set from_zone {
        from zone untrust;
        rule r1 {
            match {
                source-address 192.0.2.0/24;
                destination-address 203.0.113.203/24;
            }
            then {
                static-nat {
                    prefix {
                        192.168.1.203/24;
                    }
                }
            }
        }
    }
}
proxy-arp {
    interface ge-0/0/1.0 {
        address {
            192.0.2.1 to 192.0.2.24;
        }
```

```
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying Static NAT Configuration

Purpose

To verify that there is traffic matching the static NAT rule set.

Action

From operational mode, enter the `show security nat static rule all tenant tn1` command. View the `Translation hits` field to check for traffic that matches the rule.

```
user@host> show security nat static rule all tenant tn1
```

Sample Output

command-name

```
Total static-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Static NAT rule: r1                    Rule-set: from_zone
  Rule-Id                  : 1
```

```
  Rule position             : 1
  From zone                 : untrust
  Source addresses          : 192.0.2.0       - 192.0.2.255
  Destination addresses     : 203.0.113.203
  Host addresses            : 192.168.1.203
  Netmask                   : 32
  Host routing-instance     : N/A
  Translation hits          : 0
    Successful sessions     : 0
    Failed sessions         : 0
  Number of sessions        : 0
```

Meaning

The command output displays the static NAT rule. View the `Translation hits` field to check for traffic that matches the static rule.

Verifying Destination NAT Configuration

Purpose

To verify that there is traffic matching the destination NAT rule set.

Action

From operational mode, enter the `show security nat destination rule all tenant tn1` command. View the `Translation hits` field to check for traffic that matches the rule.

```
user@host> show security nat destination rule all tenant tn1
```

Sample Output

command-name

```
Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Destination NAT rule: r1                    Rule-set: from_zone
  Rule-Id                   : 1
  Rule position             : 1
```

```
  From zone                  : untrust
  Match
    Source addresses         : 192.0.2.0       - 192.0.2.255
    Destination addresses    : 203.0.113.202   - 203.0.113.202
  Action                     : h1
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

Meaning

The command output displays the destination NAT rule. View the `Translation hits` field to check for traffic that matches the destination rule.

Verifying Source NAT Configuration

Purpose

To verify that there is traffic matching the source NAT rule set.

Action

From operational mode, enter the `show security nat source rule all tenant tn1` command. View the `Translation hits` field to check for traffic that matches the rule.

```
user@host> show security nat source rule all tenant tn1
```

Sample Output

command-name

```
Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0
source NAT rule: r1                     Rule-set: from_intf
  Rule-Id                  : 1
  Rule position            : 1
  From interface           : ge-0/0/0.0
  To interface             : ge-0/0/1.0
```

```
Match
  Source addresses         : 192.168.1.0     - 192.168.1.255
  Destination addresses    : 203.0.113.200   - 203.0.113.200
Action                       : pat
  Persistent NAT type        : N/A
  Persistent NAT mapping type : address-port-mapping
  Inactivity timeout         : 0
  Max session number         : 0
Translation hits           : 0
  Successful sessions      : 0
  Failed sessions          : 0
Number of sessions         : 0
```

Meaning

The command output displays the source NAT rule. View the `Translation hits` field to check for traffic that matches the source rule.

RELATED DOCUMENTATION

Tenant System Configuration Overview | 533

Content Security for Tenant Systems

IN THIS SECTION

Content Security provides multiple security features and services for SRX Series Firewalls on the network, protecting users from security threats in a simplified way. Content Security secures the tenant systems from viruses, malware, or malicious attachments by scanning the incoming data using Deep Packet Inspection and prevents access to unwanted websites by installing Enhanced Web Filtering (EWF).

Understanding Content Security Features in Tenant Systems

Content Security in tenant systems provides several security features such as antispam, antivirus, content filtering, and Web filtering to secure users from multiple Internet-borne threats. The advantage of Content Security is streamlined installation and management of these multiple security capabilities. The tenant systems administrator configures the Content Security features. Configuring Content Security features for tenant systems is similar to configuring Content Security features on a device that is not configured for tenant systems.

The security features provided as part of the Content Security solution are:

- *Antispam Filtering*—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. The default antispam feature is configured at the tenant system administrator and it is applicable for all the tenant systems.
- *Content Filtering*—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. The default content filtering feature is configured at the tenant system administrator and it is applicable for all the tenant systems.
- *Web Filtering*—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. The default Web filtering feature is configured at the tenant system administrator, and the tenant system inherit these default Web filtering configuration.
- *Sophos Antivirus* —Sophos Antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. Sophos Antivirus is as an in-the-cloud antivirus solution. The default antivirus feature is configured at the tenant system administrator, and the tenant system inherit these default antivirus configuration.
- *Avira Antivirus* —Avira Antivirus feature profile settings include the scanning options, such as virus detection type, allowlist, blocklist, fallback and notification options. Only one Avira antivirus, Web filtering, Antispam filtering, or Content filtering engine is running in root system. You must configure the Avira antivirus, Web filtering, and Antispam filtering feature type in default configuration. It is configured by the root-user only. All tenants should use the same routing engine and profile type.

You must configure the custom objects for the Web filtering, anti-spam, and content filtering features before configuring the Content Security features. You can configure custom objects for each tenant system.

The predefined Content Security default policy parameters for Web filtering, content filtering, antivirus, and antispam profiles are configured at the tenant system administrator. The tenant system inherit the same antivirus and Web filtering features configured for the tenant system administrator. The options such as `mime-whitelist` and `url-whitelist` in antivirus profile, and `address-blacklist` and `address-whitelist` in antispam profile can be configured at the following hierarchy levels, respectively:

- [edit security utm feature-profile anti-virus sophos-engine profile]
- [edit security utm feature-profile anti-spam sbl profile]

The options url-whitelist and url-blacklist are not supported in the Web fiterling profile, you can use the custom category option to achieve the function.

Example: Configuring Content Security for the Tenant System

IN THIS SECTION

This example shows how to configure the Content Security features antivirus, antispam, content filtering, custom message, custom url category, and Web filtering in the tenant system. The tenant system administrator is responsible for assigning the Content Security features to the tenant system.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall configured with the tenant systems.
- Junos OS Release 19.2R1 and later releases.

Before you begin:

- Understand the tenant systems role and functions. See tenant systems overview.

Overview

The tenant system administrator assigns Content Security features antivirus, antispam, content filtering, and Web filtering to the tenant system.

This example shows how to configure the Content Security features for tenant system.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set tenants TSYS1 security utm custom-objects url-pattern cust-list value www.ask.com
set tenants TSYS1 security utm custom-objects url-pattern cust-list value www.playboy.com
set tenants TSYS1 security utm custom-objects url-pattern cust-list2 value www.baidu.com
set tenants TSYS1 security utm custom-objects custom-url-category cust-list value cust-list
set tenants TSYS1 security utm custom-objects custom-url-category cust-list2 value cust-list2
set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile my_local1
default log-and-permit
set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile my_local1
category cust-list action log-and-permit
set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile my_local1
category cust-list2 action block
set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile my_local1
fallback-settings default log-and-permit
set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced profile
ewf_my_profile1 category Enhanced_Adult_Content action block
set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced profile
ewf_my_profile1 category Enhanced_Social_Web_Facebook action log-and-permit
set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced profile
ewf_my_profile1 category cust-list action block
set tenants TSYS1 security utm utm-policy utmpolicy1 web-filtering http-profile ewf_my_profile1
```

Configuring Content Security for Tenant 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. Log in to the tenant system and enter configuration mode.

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

2. Configure the custom objects for the tenant system.

```
[edit tenants TSYS1 security utm custom-objects]
user@host# url-pattern cust-list value www.ask.com
user@host# url-pattern cust-list value www.playboy.com
user@host# url-pattern cust-list2 value www.baidu.com
user@host# custom-url-category cust-list value cust-list
user@host# custom-url-category cust-list2 value cust-list2
```

3. Configure the feature profile `web-filtering` for the tenant system.

```
[edit tenants TSYS1 security utm feature-profile]
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile
my_local1 default log-and-permit
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile
my_local1 category cust-list action log-and-permit
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile
my_local1 category cust-list2 action block
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-local profile
my_local1 fallback-settings default log-and-permit
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced
profile ewf_my_profile1 category Enhanced_Adult_Content action block
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced
profile ewf_my_profile1 category Enhanced_Social_Web_Facebook action log-and-permit
user@host# set tenants TSYS1 security utm feature-profile web-filtering juniper-enhanced
profile ewf_my_profile1 category cust-list action block
```

4. Configure the Content Security policy for the tenant system.

```
[edit tenants TSYS1 security utm ]
user@host# set tenants TSYS1 security utm utm-policy utmpolicy1 web-filtering http-profile
ewf_my_profile1
```

Results

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1 security utm custom-objects` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TSYS1 security utm custom-objects
url-pattern {
    cust-list {
        value [ www.ask.com www.playboy.com ];
    }
    cust-list2 {
        value www.baidu.com;
    }
}
custom-url-category {
    cust-list {
        value cust-list;
    }
    cust-list2 {
        value cust-list2;
    }
}
```

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1 security utm feature-profile web-filtering` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TSYS1 security utm feature-profile web-filtering
juniper-local {
    profile my_local1 {
        default log-and-permit;
        category {
            cust-list {
```

```
                action log-and-permit;
            }
            cust-list2 {
                action block;
            }
        }
        fallback-settings {
            default log-and-permit;
        }
    }
}
juniper-enhanced {
    profile ewf_my_profile1 {
        category {
            Enhanced_Adult_Content {
                action block;
            }
            Enhanced_Social_Web_Facebook {
                action log-and-permit;
            }
            cust-list {
                action block;
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1 security utm` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TSYS1 security utm
utm-policy utmpolicy1 {
    web-filtering {
        http-profile ewf_my_profile1;
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying Web Filtering Configuration

Purpose

Verify that the Web filtering feature is configured for the tenant system.

Action

From operational mode, enter the `show security utm web-filtering statistics tenant TSYS1` command to view the details of the Web filtering feature configured for the tenant system.

```
user@host> show security utm web-filtering statistics tenant TSYS1
UTM web-filtering statistics:
    Total requests:                   19784932
    white list hit:                   0
    Black list hit:                   0
    No license permit:                0
    Queries to server:                19782736
    Server reply permit:              18819472
    Server reply block:               0
```

Meaning

The output displays the Web filtering statistics for the tenant system.

IDP for Tenant Systems

IN THIS SECTION

An Intrusion Detection and Prevention (IDP) policy in tenant systems enables you to selectively enforce various attack detection and prevention techniques on the network traffic passing through an SRX Series Firewall. The SRX Series Firewalls offer the same set of IDP signatures that are available on Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to secure networks against attacks.

Understanding IDP for Tenant Systems

IN THIS SECTION

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 tenant system.

This topic includes the following sections:

IDP Policies

Configuring IDP policies at the root level and tenant systems level are similar. IDP policy templates configured at the root level are visible and used by all tenant systems. The primary administrator

specifies an IDP policy in the security profile that is bound to a tenant system. To enable IDP in a tenant system, the primary administrator or tenant system administrator configures a security policy that defines the traffic to be inspected and specifies at the `permit application-services idp-policy idp-policy-name` hierarchy level.

The primary administrator can configure multiple IDP policies and a tenant system can have multiple IDP policies at a time. For tenant systems, the primary administrator can either bind the same IDP policy to multiple tenant systems or bind the necessary IDP policies to each tenant system. If you configure more than one IDP policy, then configuring a default IDP policy is mandatory.

The primary administrator configures the number of maximum IDP sessions reservation for a primary logical system and tenant systems. The number of IDP sessions that are allowed for a primary logical system are defined using the command `set security idp max-sessions max-sessions` and the number of IDP sessions that are allowed for a tenant system are defined using the command `set security idp tenant-system tenant-system max-sessions max-sessions`.

The tenant system administrator performs the following actions:

- Configure multiple IDP policies and attach to the firewall policies to be used by the tenant systems. If the IDP policy is not configured for a tenant system, the default IDP policy configured by the primary administrator is used. The IDP policy is bound to the tenant systems through a tenant systems security policy.
- Create or modify IDP policies for their tenant system. The IDP policies are bound to tenant systems. When an IDP policy is changed, and commit fails, only the tenant system that has initiated the commit change is notified about the commit failure.
- The tenant system administrator can create security zones in the tenant system and assign interfaces to each security zone. Zones that are specific to tenant systems cannot be referenced in IDP policies configured by the primary administrator. The primary administrator can reference zones in the primary logical system in an IDP policy configured for the primary logical system.
- View the attack statistics detected and IDP counters, attack table, and policy commit status by the individual tenant system using the commands `show security idp counters`, `show security idp attack table`, `show security idp policies`, `show security idp policy-commit-status`, and `show security idp security-package-version`.

View the attack statistics detected and IDP counters, attack table, and policy commit status from the root using the commands `show security idp counters counters tenant tenant-name`, `show security idp attack table tenant tenant-name`, `show security idp policies tenant tenant-name`, `show security idp policy-commit-status tenant tenant-name`, and `show security idp security-package-version tenant tenant-name`.

Limitation

- IDP policy compilation in Packet Forwarding Engine is done at global level. Any changes in policy made for a logical system or a tenant system results in the compilation of policies of all the logical systems or tenant systems because the IDP internally treats it as a single global policy.
- Any changes in policy made for a logical system or a tenant system results in clearing the attack table of all logical systems or a tenant systems.

IDP Installation and Licensing for Tenant 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 tenant system on the device.

A single IDP security package is installed for all tenant systems on the device at the root level. 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 tenant systems.

Understanding IDP Features in Tenant Systems

IN THIS SECTION

This topic includes the following sections:

Rulebases

A single IDP policy can contain only one instance of any type of rulebase. 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.

NOTE: Status monitoring for IPS is global to the device and not on a per tenant system basis.

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 tenant systems.

Logging and Monitoring

Status monitoring options are available to the primary 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 tenant system basis.

NOTE:

- SNMP monitoring for IDP is not supported on tenant systems.
- The tenant systems supports only the stream mode for syslog and does not support the event mode.

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

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

- Attack logs. The following example shows an attack log for the `TSYS1` tenant system:

```
"<14>1 2019-02-18T02:17:56+05:30 4.0.0.254 pamba RT_IDP  - -  IDP_ATTACK_LOG_EVENT_LS: Lsys
TSYS1: IDP: At 1550485076, SIG Attack log <4.0.0.1/51480->5.0.0.1/21> for TCP protocol and
service SERVICE_IDP application FTP by rule 1 of rulebase IPS in policy new. attack: id=4641,
repeat=0, action=NONE, 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:l1z1:xe-4/0/0.0->l1z2:xe-4/0/1.0, packet-log-id: 0, alert=no, username=N/A, roles=N/A
and misc-message -
```

- IP action logs. The following example shows an IP action log for the TSYS1 tenant system:

```
"<14>1 2019-02-19T02:21:43+05:30 4.0.0.254 pamba RT_FLOW  - -  FLOW_IP_ACTION_LS: Lsys TSYS1:
Flow IP action detected attack attempt:4.0.0.1/51492 --> 5.0.0.1/21 from interface xe
-4/0/0.0, from zone l1z1, action close.
"<14>1 2019-02-19T02:21:45+05:30 4.0.0.254 pamba RT_FLOW  - -  APPTRACK_SESSION_CLOSE_LS:
Lsys TSYS1: AppTrack session closed Closed by junos-tcp-clt-emul: 4.0.0.1/51492-
>5.0.0.1/        21 junos-ftp FTP UNKNOWN 4.0.0.1/51492->5.0.0.1/21 N/A N/A 6 l1z1-l1z2 l1z1
l1z2 50000058 6(287) 5(281) 6 N/A N/A No N/A N/A VR1 xe-4/0/1.0  0 0 Infrastructure File-
Servers N/A         N/A
```

Example: Configuring IDP Policies and Attacks for Tenant Systems

IN THIS SECTION

This example shows how to configure IDP policies and attacks for tenant systems.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewall configured with the tenant systems.
- Junos OS Release 19.2R1 and later releases.

Before you configure IDP policies and attacks for tenant systems, be sure you have:

- Read "Tenant Systems Overview" on page 525 to understand how this task fits into the overall configuration process.

- Create tenant system TSYS1. See Example: Creating Tenant Systems, Tenant System Administrators, and an Interconnect VPLS Switch.
- Create security zones for tenant system TSYS1. See "Example: Configuring Zones in the Tenant System" on page 570.
- Log in to the tenant system as the tenant system administrator. See "Tenant System Configuration Overview" on page 533.

Overview

In this example you configure IDP custom attacks, policies, custom attack group, pre-defined attack and attack-group, and dynamic attack group in the tenant system TSYS1.

Configuration

IN THIS SECTION

Configuring a Custom Attack

CLI Quick Configuration

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

```
set security idp custom-attack my-http severity info
set security idp custom-attack my-http attack-type signature protocol-binding application HTTP
set security idp custom-attack my-http attack-type signature context http-get-url
set security idp custom-attack my-http attack-type signature pattern .*testing.*
set security idp custom-attack my-http attack-type signature direction any
```

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

```
[edit security idp]
user@host:TSYS1# set custom-attack my-http severity info
```

2. Configure stateful signature parameters.

```
[edit security idp]
user@host:TSYS1# set custom-attack my-http attack-type signature protocol-binding application
HTTP
user@host:TSYS1# set custom-attack my-http attack-type signature context http-get-url
user@host:TSYS1# set custom-attack my-http attack-type signature pattern .*testing.*
user@host:TSYS1# set custom-attack my-http attack-type signature direction any
```

Results

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

```
[edit]
user@host:TSYS1# show security idp custom-attack my-http
severity info;
    attack-type {
    signature {
        protocol-binding {
            application HTTP;
        }
        context http-get-url;
        pattern .*testing.*;
        direction any;
```

```
    }
}
```

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

Configuring an IDP Policy

CLI Quick Configuration

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

```
set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match application default
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-attacks my-http
set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
```

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]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match from-zone any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match source-address any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match destination-address any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match application default
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks custom-attacks my-
http
```

2. Configure actions for the IDP policy.

```
[edit security idp]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
```

Results

From configuration mode, confirm your configuration by entering the `show security idp idp-policy idpengine` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host:TSYS1# show security idp idp-policy idpengine
rulebase-ips {
    rule 1 {
        match {
            from-zone any;
            source-address any;
            to-zone any;
            destination-address any;
            application default;
            attacks {
                custom-attacks my-http;
            }
        }
        then {
            action {
                no-action;
            }
            notification {
                log-attacks;
            }
        }
    }
}
```

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

Configuring Multiple IDP Policies with a Default IDP Policy

CLI Quick Configuration

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

```
set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match application default
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks predefined-attacks
HTTP:AUDIT:URL
set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
set security idp idp-policy idpengine1 rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine1 rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine1 rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine1 rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine1 rulebase-ips rule 1 match attacks predefined-attacks
FTP:USER:ROOT
set security idp idp-policy idpengine1 rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine1 rulebase-ips rule 1 then notification log-attacks
set security policies from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match source-address any
set security policies from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match destination-address any
set security policies from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match application any
set security policies from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match dynamic-application
junos:FTP
set security policies from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 then permit application-
services idp-policy idpengine1
set security policies from-zone l1z1 to-zone l1z2 policy 2 match source-address any
set security policies from-zone l1z1 to-zone l1z2 policy 2 match destination-address any
set security policies from-zone l1z1 to-zone l1z2 policy 2 match application any
set security policies from-zone l1z1 to-zone l1z2 policy 2 match dynamic-application junos:HTTP
set security policies from-zone l1z1 to-zone l1z2 policy 2 then permit application-services idp-
policy idpengine
set security idp default-policy idpengine1
```

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 multiple IDP policies:

1. Create multiple IDP policies and configure match conditions.

```
[edit security idp]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match from-zone any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match source-address any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match destination-address any
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match application default
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks predefined-
attacks HTTP:AUDIT:URL
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 match from-zone any
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 match source-address any
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 match to-zone any
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 match destination-address any
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 match attacks predefined-
attacks FTP:USER:ROOT
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 then action no-action
user@host:TSYS1# set idp-policy idpengine1 rulebase-ips rule 1 then notification log-attacks
```

2. Configure security policies and attach IDP policies to them.

```
[edit security policies]
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match source-address any
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match destination-address
any
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match application any
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 match dynamic-application
junos:FTP
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy l1z1-l1z2 then permit application-
services idp-policy idpengine1
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy 2 match source-address any
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy 2 match destination-address any
```

```
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy 2 match application any
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy 2 match dynamic-application junos:HTTP
user@host:TSYS1# set from-zone l1z1 to-zone l1z2 policy 2 then permit application-services
idp-policy idpengine
```

3. Configure a default IDP policy.

> **NOTE**: If you configure more than one IDP policy, then configuring a default IDP policy is mandatory.

```
[edit security idp]
user@host:TSYS1# set default-policy idpengine1
```

Results

From configuration mode, confirm your configuration by entering the `show security idp idp-policy idpengine`, `show security idp idp-policy idpengine1`, `show security policies`, and `show security policies` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host:TSYS1# show security idp idp-policy idpengine
rulebase-ips {
    rule 1 {
        match {
            from-zone any;
            source-address any;
            to-zone any;
            destination-address any;
            application default;
            attacks {
                predefined-attacks HTTP:AUDIT:URL;
            }
        }
        then {
            action {
                no-action;
            }
            notification {
```

```
                log-attacks;
            }
        }
    }
}
```

```
[edit]
user@host:TSYS1# show security idp idp-policy idpengine1
rulebase-ips {
    rule 1 {
        match {
            from-zone any;
            source-address any;
            to-zone any;
            destination-address any;
            attacks {
                predefined-attacks FTP:USER:ROOT;
            }
        }
        then {
            action {
                no-action;
            }
            notification {
                log-attacks;
            }
        }
    }
}
```

```
[edit]
user@host:TSYS1# show security policies
from-zone l1z1 to-zone l1z2 {
    policy l1z1-l1z2 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application junos:FTP;
        }
```

```
        then {
            permit {
                application-services {
                    idp-policy idpengine1;
                }
            }
        }
    }
    policy 2 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application junos:HTTP;
        }
        then {
            permit {
                application-services {
                    idp-policy idpengine;
                }
            }
        }
    }
}
```

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

Configuring IDP Custom Attack Group

CLI Quick Configuration

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

```
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-attack-groups
cust-group
set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-attacks
set security idp custom-attack customftp severity warning
set security idp custom-attack customftp attack-type signature context ftp-username
set security idp custom-attack customftp attack-type signature pattern .*guest.*
```

```
set security idp custom-attack customftp attack-type signature direction client-to-server
set security idp custom-attack-group cust-group group-members customftp
set security idp custom-attack-group cust-group group-members ICMP:INFO:TIMESTAMP
set security idp custom-attack-group cust-group group-members "FTP - Minor"
set security idp custom-attack-group cust-group group-members dyn1
set security idp dynamic-attack-group dyn1 filters category values HTTP
```

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 IDP custom attack group:

1. Create the IDP policy.

```
[edit security idp]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks custom-attack-
groups cust-group
```

2. Configure match condition of IDP policy.

```
[edit security idp]
user@host:TSYS1# set security idp idp-policy idpengine rulebase-ips rule 1 then action no-
action
user@host:TSYS1# set security idp idp-policy idpengine rulebase-ips rule 1 then notification
log-attacks
```

3. Configure stateful signature parameters.

```
[edit security idp]
user@host:TSYS1# set security idp custom-attack customftp severity warning
user@host:TSYS1# set custom-attack customftp attack-type signature context ftp-username
user@host:TSYS1# set custom-attack customftp attack-type signature pattern .*guest.*
user@host:TSYS1# set custom-attack customftp attack-type signature direction client-to-server
user@host:TSYS1# set custom-attack-group cust-group group-members customftp
user@host:TSYS1# set custom-attack-group cust-group group-members ICMP:INFO:TIMESTAMP
user@host:TSYS1# set custom-attack-group cust-group group-members "FTP - Minor"
```

```
user@host:TSYS1# set custom-attack-group cust-group group-members dyn1
user@host:TSYS1# set dynamic-attack-group dyn1 filters category values HTTP
```

Results

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

```
[edit]
user@host:TSYS1# show security idp
idp-policy idpengine {
    rulebase-ips {
        rule 1 {
            match {
                attacks {
                    custom-attack-groups cust-group;
                }
            }
            then {
                action {
                    no-action;
                }
                notification {
                    log-attacks;
                }
            }
        }
    }
}
custom-attack customftp {
    severity warning;
    attack-type {
        signature {
            context ftp-username;
            pattern .*guest.*;
            direction client-to-server;
        }
    }
}
custom-attack-group cust-group {
```

```
    group-members [ customftp ICMP:INFO:TIMESTAMP "FTP - Minor" dyn1 ];
}
dynamic-attack-group dyn1 {
    filters {
        category {
            values HTTP;
        }
    }
}
```

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

Configuring Pre-defined Attack and Attack Group

CLI Quick Configuration

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

```
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks predefined-attacks
FTP:USER:ROOT
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks predefined-attack-groups
"HTTP - All"
```

Step-by-Step Procedure

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

To configure the pre-defined attack and attack group:

1. Configure the pre-defined attack.

```
[edit security idp]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks predefined-
attacks FTP:USER:ROOT
```

2. Configure the pre-defined attack group.

```
[edit security idp]
user@host:TSYS1# set idp-policy idpengine rulebase-ips rule 1 match attacks predefined-attack-
groups "HTTP - All"
```

Results

From configuration mode, confirm your configuration by entering the `show security idp idp-policy idpengine` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host:TSYS1# show security idp idp-policy idpengine
rulebase-ips {
    rule 1 {
        match {
            attacks {
                predefined-attacks FTP:USER:ROOT;
                predefined-attack-groups "HTTP - All";
            }
        }
        then {
            action {
                no-action;
            }
            notification {
                log-attacks;
            }
        }
    }
}
```

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

Configuring IDP Dynamic Attack Group

CLI Quick Configuration

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

```
set security idp dynamic-attack-group dyn1 filters direction values server-to-client
```

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 IDP dynamic attack group:

1. Configure dynamic attack group parameter.

```
[edit security idp]
user@host:TSYS1# set dynamic-attack-group dyn1 filters direction values server-to-client
```

Results

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

```
[edit]
user@host:TSYS1# show security idp
dynamic-attack-group dyn1 {
    filters {
        direction {
            values server-to-client;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verify IDP Policies and Commit Status

Purpose

Verify that the IDP policies and commit status is displayed after policy compilation for the tenant system TSYS1.

Action

From operational mode, enter the `show security idp policies` command.

```
user@host:TSYS1> show security idp policies
ID    Name                  Sessions    Memory      Detector
 1     idpengine             0           186024      12.6.130180122
```

From operational mode, enter the `show security idp policy-commit-status` command.

```
user@host:TSYS1> show security idp policy-commit-statusIDP policy[/var/db/idpd/bins//idp-policy-
unified.bin.gz.v] and detector[/var/db/idpd/sec-repository/installed-detector/libidp-
detector.so.tgz.v] loaded successfully.
The loaded policy size is:2912 Bytes
```

Meaning

The output displays the IDP policy configured in the tenant system TSYS1 and the commit status information.

Verify IDP Attack Detection

Purpose

Verify that the IDP attack detection is successful for the tenant system TSYS1 and displayed in the attack table.

Action

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

```
user@host:TSYS1> show security idp attack table
IDP attack statistics:
  Attack name                                #Hits
  my-http                                        1
```

Meaning

The output displays the attacks detected for the custom attack that is configured in the tenant system TSYS1.

Verify IDP Counters

Purpose

Verify one of the IDP counter status is displayed for the tenant system TSYS1.

Action

From operational mode, enter the show security idp counters flow command.

```
user@host:TSYS1> show security idp counters flow
IDP counters:

  IDP counter type                                                  Value
Fast-path packets                                                   38
Slow-path packets                                                   1
Session construction failed                                         0
Session limit reached                                               0
Session inspection depth reached                                    0
```

```
Memory limit reached                                                0
Not a new session                                                   0
Invalid index at ageout                                             0
Packet logging                                                      0
Policy cache hits                                                   0
Policy cache misses                                                 1
Policy cache entries                                                0
Maximum flow hash collisions                                        0
Flow hash collisions                                                0
Gates added                                                         0
Gate matches                                                        0
Sessions deleted                                                    1
Sessions aged-out                                                   0
Sessions in-use while aged-out                                      0
TCP flows marked dead on RST/FIN                                    1
Policy init failed                                                  0
Policy reinit failed                                                0
Number of times Sessions exceed high mark                           0
Number of times Sessions drop below low mark                        0
Memory of Sessions exceeds high mark                                0
Memory of Sessions drops below low mark                             0
SM Sessions encountered memory failures                             0
SM Packets on sessions with  memory failures                        0
IDP session gate creation requests                                  0
IDP session gate creation acknowledgements                          0
IDP session gate hits                                               0
IDP session gate timeouts                                           0
Number of times Sessions crossed the CPU threshold value that is set    0
Number of times Sessions crossed the CPU upper threshold            0
Sessions constructed                                                1
SM Sessions ignored                                                 0
SM Sessions dropped                                                 0
SM Sessions interested                                              2
SM Sessions not interested                                          0
SM Sessions interest error                                          0
Sessions destructed                                                 1
SM Session Create                                                   1
SM Packet Process                                                   38
SM ftp data session ignored by idp                                  1
SM Session close                                                    1
SM Client-to-server packets                                         15
SM Server-to-client packets                                         23
SM Client-to-server L7 bytes                                        99
```

SM Server-to-client L7 bytes	367
Client-to-server flows ignored	0
Server-to-client flows ignored	0
Server-to-client flows tcp optimized	0
Client-to-server flows tcp optimized	0
Both directions flows ignored	1
Fail-over sessions dropped	0
Sessions dropped due to no policy	0
IDP Stream Sessions dropped due to memory failure	0
IDP Stream Sessions ignored due to memory failure	0
IDP Stream Sessions closed due to memory failure	0
IDP Stream Sessions accepted	0
IDP Stream Sessions constructed	0
IDP Stream Sessions destructed	0
IDP Stream Move Data	0
IDP Stream Sessions ignored on JSF SSL Event	0
IDP Stream Sessions not processed for no matching rules	0
IDP Stream stbuf dropped	0
IDP Stream stbuf reinjected	0
Busy pkts from stream plugin	0
Busy pkts from pkt plugin	0
bad kpp	0
Lsys policy id lookup failed sessions	0
NGAppID Events with no L7 App	0
NGAppID Events with no active-policy	0
NGAppID Detector failed from event handler	0
NGAppID Detector failed from API	0
Busy packets	0
Busy packet Errors	0
Dropped queued packets (async mode)	0
Dropped queued packets failed(async mode)	0
Reinjected packets (async mode)	0
Reinjected packets failed(async mode)	0
AI saved processed packet	0
busy packet count incremented	0
busy packet count decremented	0
session destructed in pme	0
session destruct set in pme	0
kq op hold	0
kq op drop	0
kq op route	0
kq op continue	37
kq op error	0

```
kq op stop                                                          0
PME wait not set                                                    0
PME wait set                                                        0
PME KQ run not called                                               0
IDP sessions ignored for content decompression in intel inspect mode    0
IDP sessions ignored for bytes depth limit in intel inspect mode        0
IDP sessions ignored for protocol decoding in intel inspect mode        0
IDP sessions detected CPU usage crossed intel inspect CPU threshold     0
IDP sessions detected mem drop below intel inspect low mem threshold    0
```

Meaning

The output displays the IDP counter flow status is displayed properly for the tenant system TSYS1.

ALG for Tenant Systems

IN THIS SECTION

An Application Layer Gateway (ALG) in tenant systems enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server. ALGs supports the applications such as Transfer Protocol (FTP) and various IP protocols that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. For more information, see the following topics:

Understanding ALG Support for Tenant System

An Application Layer Gateway (ALG) enables the gateway to parse application layer payloads and take decisions whether to allow or deny traffic to the application server.

Starting in Junos OS Release 18.3R1, the ALG feature supported on logical systems is now extended on tenants systems.

The tenant systems administrator can configure the ALG features for the tenant systems. The primary administrator can configure the ALG features and display the ALG information for all tenants. The tenant systems administrator can only apply configurations and display information in its own tenant.

Each tenant system displays the ALG counters to monitor the traffic. For example, use commands `show security alg sip counters tenants TN1` to get SIP counters in tenant systems and `show security alg sip counters tenants all` to get SIP counters in all existing tenant systems.

Enabling the security log for the tenant generates the ALG logs per tenant.

NOTE: When you upgrade to Junos OS Release 18.3R1, the ALG status for each tenant system might be different depending on the default configuration or configuration in a release prior to Junos OS Release 18.3R1. We recommend you to change the ALG configurations for tenant systems as per your requirements after an upgrade to latest Junos OS version.

Enabling and Disabling ALG for Tenant System

This topic shows how to enable or disable the ALG status for each tenant system.

1. By Default IKE ALG is disabled on the tenant system. To enable this ALG, use the following command.
   - Enable IKE and ESP ALG with NAT.

```
[edit]
user@host# set tenants TN1 security alg ike-esp-nat enable
```

2. By default, the DNS, FTP, PPTP, SIP, SUNRPC and TWAMP ALGs are enabled on the tenant system. To disable these ALGs, use the following commands.
   - Disable DNS ALG.

```
[edit]
user@host# set tenants TN1 security alg dns disable
```

- Disable FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp disable
```

- Disable H323 ALG.

```
[edit]
user@host# set tenants TN1 security alg h323 disable
```

- Disable MGCP ALG.

```
[edit]
user@host# set tenants TN1 security alg mgcp disable
```

- Disable MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc disable
```

- Disable PPTP ALG.

```
[edit]
user@host# set tenants TN1 security alg pptp disable
```

- Disable RSH ALG.

```
[edit]
user@host# set tenants TN1 security alg rsh disable
```

- Disable RTSP ALG.

```
[edit]
user@host# set tenants TN1 security alg rtsp disable
```

- Disable SCCP ALG.

```
[edit]
user@host# set tenants TN1 security alg sccp disable
```

- Disable SIP ALG.

```
[edit]
user@host# set tenants TN1 security alg sip disable
```

- Disable SQL ALG.

```
[edit]
user@host# set tenants TN1 security alg sql disable
```

- Disable SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc disable
```

- Disable TALK ALG.

```
[edit]
user@host# set tenants TN1 security alg talk disable
```

- Disable TFTP ALG.

```
[edit]
user@host# set tenants TN1 security alg tftp disable
```

3. Configuring ALG functions in tenant systems.

- Configure DNS ALG.

```
[edit]
user@host# set tenants TN1 security alg dns
```

- Configure FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp
```

- Configure H323 ALG.

```
[edit]
user@host# set tenants TN1 security alg h323
```

- Configure IKE and ESP ALG with NAT.

```
[edit]
user@host# set tenants TN1 security alg ike-esp-nat
```

- Configure MGCP ALG.

```
[edit]
user@host# set tenants TN1 security alg mgcp
```

- Configure MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc
```

- Configure PPTP ALG.

```
[edit]
user@host# set tenants TN1 security alg pptp
```

- Configure RSH ALG.

```
[edit]
user@host# set tenants TN1 security alg rsh
```

- Configure RTSP ALG.

```
[edit]
user@host# set tenants TN1 security alg rtsp
```

- Configure SCCP ALG.

```
[edit]
user@host# set tenants TN1 security alg sccp
```

- Configure SIP ALG.

```
[edit]
user@host# set tenants TN1 security alg sip
```

- Configure SQL ALG.

```
[edit]
user@host# set tenants TN1 security alg sql
```

- Configure SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc
```

- Configure TALK ALG.

```
[edit]
user@host# set tenants TN1 security alg talk
```

- Configure TFTP ALG.

```
[edit]
user@host# set tenants TN1 security alg tftp
```

- Configure TWAMP ALG.

```
[edit]
user@host# set tenants TN1 security alg twamp
```

- Configure extended function for FTP ALG.

```
[edit]
user@host# set tenants TN1 security alg ftp allow-mismatch-ip-address
```

- Configure extended function for MSRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg msrpc map-entry-timeout 10
```

- Configure extended function for SUNRPC ALG.

```
[edit]
user@host# set tenants TN1 security alg sunrpc map-entry-timeout 10
```

- Configure extended function for SIP ALG.

```
[edit]
user@host# set tenants TN1 security alg sip retain-hold-resource
```

Example: Configuring ALG in Tenant System

IN THIS SECTION

This example shows how to configure ALGs in tenant system and send traffic based on FTP ALG configuration of the tenant system individually.

Requirements

This example uses the following hardware and software components:

- An SRX device
- Junos OS Release 18.3R1

Before you begin:

- Read the ALG Support for Tenant System to understand how and where this procedure fits in the overall tenant support for ALGs.

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

Overview

In this example, the ALG for FTP is configured to monitor and allow FTP traffic to be exchanged between the clients and the server on a tenant system.

By default, the FTP ALG is enabled on the tenant system.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50
set tenants TN1 routing-instances VR_TN1 instance-type vpls
set tenants TN1 routing-instances VR_TN1 interface lt-0/0/0.0
set system security-profile p1 tenant TN1
set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic system-services all
set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic protocols all
set tenants TN1 security zones security-zone TN1_Czone interfaces ge-0/0/0
set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic system-services all
set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic protocols all
set tenants TN1 security zones security-zone TN1_Szone interfaces ge-0/0/1
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 match source-
address any
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 match
destination-address any
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 match
application junos-ftp
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 match
application junos-ping
set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11 then permit
set tenants TN1 security policies default-policy deny-all
```

Configuring FTP ALG in a Tenant 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.

To configure an ALG on a tenant system:

1. Configure a security profile p1 for tenant.

```
[edit]
set system security-profile p1 policy maximum 100
set system security-profile p1 policy reserved 50
set system security-profile p1 zone maximum 100
set system security-profile p1 zone reserved 50
set system security-profile p1 flow-session maximum 6291456
set system security-profile p1 flow-session reserved 50
set system security-profile p1 flow-gate maximum 524288
set system security-profile p1 flow-gate reserved 50
```

2. Configure interfaces and routing instances to the TN1.

```
[edit]
user@host# set tenants TN1 routing-instances VR_TN1 instance-type vpls
user@host# set tenants TN1 routing-instances VR_TN1 interface lt-0/0/0.0
```

3. Configure a security profile p1 and assign it to the tenant system TN1.

```
[edit]
user@host# set system security-profile p1 tenant TN1
```

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

```
[edit]
user@host# set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic system-
services all
user@host# set tenants TN1 security zones security-zone TN1_Czone host-inbound-traffic
protocols all
user@host# set tenants TN1 security zones security-zone TN1_Czone interfaces ge-0/0/0
user@host# set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic system-
services all
user@host# set tenants TN1 security zones security-zone TN1_Szone host-inbound-traffic
protocols all
user@host# set tenants TN1 security zones security-zone TN1_Szone interfaces ge-0/0/1
```

5. Configure a security policy that permits FTP traffic from the TN1_Czone to-zone TN1_Szone.

```
[edit]
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match source-address any
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match destination-address any
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match application junos-ftp
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
match application junos-ping
user@host# set tenants TN1 security policies from-zone TN1_Czone to-zone TN1_Szone policy p11
then permit
user@host# set tenants TN1 security policies default-policy deny-all
```

Results

From configuration mode, confirm your configuration by entering the `show tenants TN1` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TN1
    routing-instances {
        VR_TN1 {
            instance-type vpls;
            interface lt-0/0/0.0;
        }
    }
    security {
        policies {
            from-zone TN1_Czone to-zone TN1_Szone {
                policy p11 {
                    match {
                        source-address any;
                        destination-address any;
                        application [ junos-ftp junos-ping ];
                    }
                    then {
                        permit;
                    }
                }
```

```
            }
            default-policy {
                deny-all;
            }
        }
        zones {
            security-zone TN1_Czone {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
                interfaces {
                    ge-0/0/0.0;
                }
            }
            security-zone TN1_Szone {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
                interfaces {
                    ge-0/0/1.0;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying Intra-Tenant System traffic on ALG

Purpose

Verify the information about active resources, clients, groups, and sessions created through the resource manager.

Action

From operational mode, enter the `show security resource-manager summary` command.

```
user@host> show security resource-manager summary
Active resource-manager clients   : 0
Active resource-manager groups    : 0
Active resource-manager resources : 0
Active resource-manager sessions  : 0
```

Meaning

The output displays summary information about active resources, clients, groups, and sessions created through the resource manager.

Verify ALG status for Tenant System

Purpose

Verify the ALG status for tenant on the device.

Action

To verify the configuration is working properly, enter the `show security alg status tenant TN1` command.

```
user@host>show security alg status tenant TN1
ALG Status:
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Disabled
  SQL      : Disabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
  TWAMP    : Disabled
```

Meaning

The output display the alg status for FTP Enabled for the tenant system TN1.

RELATED DOCUMENTATION

Tenant Systems Overview | 525

DHCP for Tenant Systems

IN THIS SECTION

Understanding DHCP support for Tenant Systems

Starting in Junos OS Release 18.4R1, a tenant system supports the DHCP client feature to learn IP addresses for interfaces assigned to the tenant systems. Additionally, starting in Junos OS Release 18.4R1, tenant systems support the DHCP relay feature. A DHCP relay agent forwards DHCP requests and responses between the DHCP client and the DHCP server.

An interface of an SRX Series Firewall operating as a DHCP client receives the TCP or IP settings and the IP address from an external DHCP server.

An SRX Series Firewall operating as a DHCP relay agent for tenant systems forwards incoming requests from the DHCP clients to a specified DHCP server. The client requests pass through interfaces on the tenant systems.

Minimum DHCPv6 Relay Agent Configuration for Tenant Systems

The following example describes the minimum configuration required to configure an SRX Series Firewall as a DHCPv6 relay agent for the tenant system.

Before you begin determine the following:

- The DHCP routing instance name, the DHCP relay group and the DHCP active server-group for the tenant system.

1. Create a DHCPv6 relay group that includes at least one interface for the tenant system.

```
user@host# set tenants TSYS1 routing-instances R1 interface ge-0/0/0.0
```

2. Specify the DHCP group and add interfaces belonging to the group.

```
user@host# set tenants TSYS1  routing-instances R1 forwarding-options dhcp-relay dhcpv6 group
inf interface ge-0/0/0.0
```

3. Specify the name of the server-group and add the IP address for the DHCP servers belonging to the same group.

```
user@host# set tenants TSYS1  routing-instances R1 forwarding-options dhcp-relay dhcpv6
server-group server6 2001:db8::1/64
```

4. Specify the name of the active server-group.

```
user@host# set tenants TSYS1  routing-instances R1 forwarding-options dhcp-relay dhcpv6
active-server-group server6
```

5. Confirm your configuration by entering the `show tenants TSYS1 routing-instances R1` command.

```
[edit]
user@host# show tenants TSYS1 routing-instances R1
forwarding-options {
    dhcp-relay {
        dhcpv6 {
            group inf {
                interface ge-0/0/0.0;
            }
            server-group {
                server6 {
                    2001:db8::1/64;
                }
            }
            active-server-group server6;
        }
    }
}
```

Example: Configuring a DHCPv6 Client for Tenant Systems

IN THIS SECTION

This example shows how to configure a device as a DHCPv6 client for tenant systems.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall
- Junos OS Release 18.4R1

Before you begin:

- Read the Understanding DHCP support for Tenant Systems to understand how and where this procedure fits in the overall tenant systems support for DHCP.

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

Overview

In this example, a tenant system administrator configures an SRX Series Firewall as a DHCPv6 client for a tenant system.

The DHCPv6 client for a tenant system includes the following features:

- Identity association for non-temporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Autoconfig or stateful mode
- DHCP unique identifier (DUID)

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set tenants TSYS1 security zones security-zone trust host-inbound-traffic system-services all
set tenants TSYS1 security zones security-zone trust host-inbound-traffic protocols all
set tenants TSYS1 security zones security-zone trust interfaces ge-0/0/0.0
set tenants TSYS1 routing-instances r1 instance-type virtual-router
set tenants TSYS1 routing-instances r1 interface ge-0/0/0.0
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type stateful
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-
type duid-ll
set tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
set protocols router-advertisement interface ge-0/0/0.0
```

Configuring DHCPv6 Client in a Tenant System

Procedure

Step-by-Step Procedure

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

1. Configure security zones to permit traffic for a tenant system.

```
[edit tenants TSYS1 security zones]
user@host# set security-zone trust host-inbound-traffic system-services all
user@host# set security-zone trust host-inbound-traffic protocols all
user@host# set security-zone trust interfaces ge-0/0/0.0
```

2. Create a routing instance and assign the routing instance type to a tenant system.

```
[edit tenants TSYS1]
user@host# set routing-instances r1 instance-type virtual-router
```

3. Specify the interface name for the routing instance.

```
[edit tenants TSYS1]
user@host# set routing-instances r1 interface ge-0/0/0.0
```

4. Configure the DHCPv6 client type. The client type can be `autoconfig` or `stateful` for a tenant system.

   - To enable DHCPv6 auto configuration mode, configure the client type as `autoconfig`.

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

   - For stateful address assignment, configure the client type as `stateful`.

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type stateful
```

5. Specify the identity association type.

- To configure identity association for nontemporary address (IA_NA) assignment, specify the `client-ia type` as `ia-na`.

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

- To configure identity association for prefix delegation (IA_PD), specify the `client-ia-type` as `ia-pd`.

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

6. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type for the tenant system. The following DUID type is supported:

   - Link Layer address (duid-ll)

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

7. Specify the DHCPv6 client requested option as `dns-server` for the tenant system.

```
[edit tenants TSYS1 interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set req-option dns-server
```

8. Configure the router advertisement.

```
[edit]
user@host# set protocols router-advertisement interface ge-0/0/0.0
```

Results

- From configuration mode, confirm your configuration by entering the `show tenants TSYS1` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TSYS1
interfaces {
```

```
    ge-0/0/0 {
        unit 0 {
            family inet6 {
                dhcpv6-client {
                    client-type stateful;
                    client-ia-type ia-na;
                    client-ia-type ia-pd;
                    client-identifier duid-type duid-ll;
                    req-option dns-server;
                }
            }
        }
    }
}
routing-instances {
    r1 {
        instance-type virtual-router;
        interface ge-0/0/0.0;
    }
}
security {
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
    }
}
```

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

```
user@host# show protocols
router-advertisement {
    interface ge-0/0/0.0;
}
```

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

Verification

IN THIS SECTION

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

Verifying the DHCPv6 Client for the Tenant System

Purpose

Verify that the DHCPv6 client information is configured.

Action

From the operational mode, enter the `show dhcpv6 client binding tenant TSYS1` command.

```
user@host> show dhcpv6 client binding  tenant TSYS1
IP/prefix      Expires     State      ClientType     Interface      Client DUID
         2000::17/128    67762    BOUND      STATEFUL         ge-0/0/6.0
LL0x3-10:0e:7e:49:25:86
```

```
          2000:100::/64   67762    BOUND      STATEFUL         ge-0/0/6.0
LL0x3-10:0e:7e:49:25:86
```

Meaning

The output displays the address binding information for the tenant system.

Verifying the DHCPv6 Client Binding for the Tenant System

Purpose

Verify that the DHCPv6 client binding information is configured.

Action

From the operational mode, enter the `show dhcpv6 client binding detail tenant TSYS1` command.

```
user@host> show dhcpv6 client binding detail tenant TSYS1
Client Interface/Id: ge-0/0/6.0
     Hardware Address:             10:0e:7e:49:25:86
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
     ClientType                    STATEFUL
     Lease Expires:                2018-11-09 07:11:47 UTC
     Lease Expires in:             67760 seconds
     Lease Start:                  2018-11-08 07:11:47 UTC
     Bind Type:                    IA_NA IA_PD
     Preferred prefix length       0
     Sub prefix length             0
     Client DUID:                  LL0x3-10:0e:7e:49:25:86
     Rapid Commit:                 Off
     Server Identifier:            fe80::46f4:77ff:fed6:670a
     Client IP Address:            2000::17/128
     Client IP Prefix:             2000:100::/64

     DHCP options:
     Name: server-identifier, Value: VENDOR0x00000583-0x34343a34
```

Meaning

The output displays the detailed client binding information for the tenant system.

Verifying the DHCPv6 Client Statistics Information for the Tenant System

Purpose

Verify that the DHCP client statistics information is configured.

Action

From the operational mode, enter the `show dhcpv6 client statistics tenant TSYS1` command.

```
user@host> show dhcpv6 client statistics tenant TSYS1 routing-instance R1
Dhcpv6 Packets dropped:
    Total               3
    Bad Send            3

    Messages received:
    DHCPV6_ADVERTISE           1
    DHCPV6_REPLY               1
    DHCPV6_RECONFIGURE         0

    Messages sent:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             1
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             1
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
```

Meaning

The output displays the information about the number of packets discarded, the number of messages received and the number of messages sent by the DHCP client for the tenant system.

Security Log for Tenant Systems

IN THIS SECTION

Security logs for tenant systems include security events to control system's data planes. Security logs are sent in binary format to an external server from a tenant system interface. Security logs are generated per tenant system.

Understanding of Security Log for Tenant Systems

Junos OS generates separate log messages to record events that occur on the system's control and data planes. The data plane logs, also called security logs, primarily include security events that are handled inside the data plane. Security logs can be in text or binary format and they can be saved locally (event mode) or sent to an external server (stream mode). The binary format is required for stream mode and recommended to conserve log space in event mode.

If you configure security logs per tenant, then security logs are generated per tenant.

Security logs for a tenant system are sent from a tenant system interface. You can configure the assigned routing instances and the interfaces that belong to the routing tables within a tenant system.

A security profile should be defined with the number of maximum and reserved policies when you configure the stream number for a tenant system. The primary administrator can use the security profiles to specify resource allocation.

If a tenant 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 and not allocated to other tenant systems. The maximum allowed quota for stream number specifies the portion of the free global

resources that the tenant system can use. The maximum allowed quota does not ensure that the amount specified for the resource in the security profile is available. A reserved quota ensures that the resource amount specified is always available to the tenant system. Table 39 on page 734 shows the comparison of logging stream number capacity.

Table 39: Comparison of Logging Stream Number

Platform	Logging Stream Number Capacity for Tenant System + Logical System	Reserved Logging Stream Number Quota for Tenant System	Maximum Allowed Stream Number Quota for Tenant System	Maximum Allowed Stream Number Quota for Global
SRX5400, SRX5600, and SRX5800	64	0	8	64
SRX4600	300	0	8	600
SRX4100 and 4200	200	0	8	400
SRX1500	50	0	8	100

If a device is configured for a tenant system, security logs generated within the context have the **_LS** suffix in the log name, which is the same as the logical system. The following security log shows the attributes of the RT_FLOW_SESSION_CLOSE_LS log for a device that is configured for a tenant system:

```
<14>1 2018-03-12T22:50:09.596Z user RT_FLOW_SESSION_CLOSE_LS [junos@2636.1.1.1.2.137 logical-
system-name="TSYS1" reason="Some reason" source-address="192.0.2.1" source-port="7000"
destination-address="198.51.100.2" destination-port="32768" connection-tag="0" service-
name="Fake service" nat-source-address="192.0.2.1" nat-source-port="7000" nat-destination-
address="198.51.10    0.2" nat-destination-port="32768" nat-connection-tag="0" src-nat-rule-
type="Fake src nat rule" src-nat-rule-name="Fake src nat rule" dst-nat-rule-type="Fake dst nat
rule" dst-nat-rule-name="Fake dst nat rule" protocol-id="17" policy-name="Fake policy" source-
zone-name="Fake src zone" destination-zone-name="Fake dst zone" session-id-32="1" packets-from-
client="4294967295" bytes-from-client="4294967293" packets-from-server="4294967294" bytes-from-
server="4294967292" elapsed-time="4294967291" application="Fake application" nested-
application="Fake nested application" username="Fake username" roles="Fake UAC roles" packet-
incoming-interface="Fake packet incoming if" encrypted="Fake info telling if the traffic is
encrypted" application-category="Fake application category" application-sub-category="Fake
application subcategory" application-risk="-1"]
```

In the above example, security log includes **TSYS1** as the first attribute.

Starting in Junos OS Release 19.1R1, on-box reporting configurations are supported for each tenant system and logs are handled based on these configurations. Configure the `set security log report` and `set security log mode stream` commands to enable the on-box reporting. The on-box reporting feature with stream mode is also supported on tenant systems.

You can view Syslog messages in the System Log Explorer.

Example: Configure Security Log for Tenant Systems

IN THIS SECTION

This example shows how to configure security logs for a tenant system.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall.
- Junos OS Release 18.3R1 and later releases.

Before you begin:

- Understand how to configure a tenant system with security profiles for the primary logical system and two tenant systems. See Figure 1
-

Overview

SRX Series Firewalls have two types of log: system logs and security logs. System logs record control plane events, for example, admin login to the device. Security logs, also known as traffic logs, record

data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy.

The two types of logs can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

For off-box logging, security logs for a tenant system are sent from a tenant system interface. If the tenant system interface is already configured in a routing instance, then configure `routing-instance` *routing-instance-name* at `edit tenants` *tenant-name* `security log stream` *log-stream-name* `host` hierarchy. If the interface is not configured in routing instance, then no routing instance should be configured at `set tenants` *tenant-name* `security log stream` *log-stream-name* `host` hierarchy.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set tenants TSYS1 security log mode stream
set tenants TSYS1 security log stream TN1_s format binary host 1.3.54.22
set tenants TSYS1 security log source-address 2.3.45.66
set tenants TSYS1 security log transport protocol tls
set tenants TSYS1 routing-instances TN1_ri instance-type virtual-router
set tenants TSYS1 routing-instances TN1_ri interface ge-0/0/3
set tenants TSYS1 security log stream TN1_s host routing-instance TN1_ri
set system security-profile p1 security-log-stream-number reserved 1
set system security-profile p1 security-log-stream-number maximum 2
set system security-profile p1 tenant TSYS1
```

Procedure

Step-by-Step Procedure

The following procedure specifies how to configure security logs for a tenant system.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging.

```
[edit ]
user@host# set tenants TSYS1 security log mode stream
user@host# set tenants TSYS1 security log stream TN1_s format binary host 1.3.54.22
```

2. For off-box security logging, specify the source address, which identifies the SRX Series Firewall that generated the log messages. The source address is required.

```
[edit ]
user@host# set tenants TSYS1 security log source-address 2.3.45.66
```

3. Specify the routing instance and define the interface.

```
[edit ]
user@host# set tenants TSYS1 routing-instances TN1_ri instance-type virtual-router
user@host# set tenants TSYS1 routing-instances TN1_ri interface ge-0/0/3
```

4. Define routing instance for a tenant system. If the interface is already configured in routing instance, then configure `routing-instance` *`routing-instance-name`* at `edit tenants` *`tenant-name`* `security log stream` *`log-stream-name`* `host` hierarchy. If the interface is not configured in routing instance, then no routing instance should be configured at `set tenants` *`tenant-name`* `security log stream` *`log-stream-name`* `host` hierarchy.

```
[edit ]
user@host# set tenants TSYS1 security log stream TN1_s host routing-instance TN1_ri
```

5. Specify the security log transport protocol for the device.

```
[edit ]
user@host# set tenants TSYS1 security log transport protocol tls
```

Procedure

Step-by-Step Procedure

The following procedure specifies how to configure a security profile for a tenant system.

1. Configure a security profile and specify the number of maximum and reserved policies.

```
[edit ]
user@host# set system security-profile p1 security-log-stream-number reserved 1
user@host# set system security-profile p1 security-log-stream-number maximum 2
```

2. Assign the configured security profile to TSYS1.

```
[edit ]
user@host# set system security-profile p1 tenant TSYS1
```

Results

From configuration mode, confirm your configuration by entering the `show system security-profile`, `show tenants TSYS1 security log`, and `show tenants TSYS1 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 tenants TSYS1 security log
mode stream;
source-address 2.3.45.66;
transport {
    protocol tls;
}
stream TN1_s {
    format binary;
    host {
        1.3.54.22;
        routing-instance TN1_ri;
```

```
    }
}
```

```
[edit]
user@host# show tenants TSYS1 routing-instances
TN1_ri {
    instance-type virtual-router;
    interface ge-0/0/3.0;
}
```

```
[edit]
user@host# show system security-profile
p1 {
    security-log-stream-number {
        maximum 2;
        reserved 1;
    }
    tenant TSYS1;
}
```

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

Verification

IN THIS SECTION

Verifying Detailed Output for Security Log

Purpose

Verify that the output displays the resource information for all tenant systems.

Action

From operational mode, enter the `show system security-profile security-log-stream-number tenant all` command.

```
logical-system tenant name  security profile name  usage    reserved    maximum

root-logical-system         Default-Profile          0          0         8
TSYS1                       p1                       1          1         2
```

Meaning

The output displays the resource information for tenant systems.

Understanding On-Box Reporting for Tenant Systems

Starting in Junos OS Release 19.1R1, on-box reporting configurations are supported for tenant systems and logs are handled based on these configurations.

Stream mode is a set of logging services that includes:

- Off-box logging (SRX Series)
- On-box logging and reporting (SRX1500, SRX4100, SRX4200, and SRX4600 Series)

Per tenant system configuration is supported for the off-box logging and logs are handled based on these configurations. The tenant system logs for off-box logging can only be generated from the tenant system interface.

On-box reporting mechanism is an enhancement to the existing logging functionality. The existing logging functionality is modified to collect system traffic logs, analyzes the logs, and generate reports of these logs. On-box reporting feature is intended to provide a simple and easy to use interface for viewing security logs.

Configure the `set security log report` and `set security log mode stream` commands to enable the on-box reporting feature on the device for tenant systems. The on-box reporting feature with stream mode is also supported on tenant systems.

The on-box reporting feature supports:

- Generating reports based on the requirements. For example: count or volume of the session, types of logs for activities such as IDP, Content Security, and IPsec VPN.
- Capturing real-time events within a specified time range.
- Capturing all the network activities in a logical, organized, and easy-to-understand format based on various CLI specified conditions.

Configuring On-Box Reporting for Tenant Systems

SRX Series Firewalls supports different types of reports for tenant system users.

Reports are stored locally on the SRX Series Firewall and there is no requirement for separate devices or tools for logs and reports storage. The on-box reports provides a simple and easy-to-use interface for viewing the security logs.

Before you begin:

- Understand how to configure security log for tenant systems. See Example: Configure Security Log for Tenant Systems.

To configure on-box reporting for tenant system:

1. Define the tenant system name as TSYS1.

```
user@host# set tenants TSYS1
```

2. Create report within security log per tenant system.

```
user@host# set tenants TSYS1 security log report
```

3. Confirm your configuration by entering the `show tenants TSYS1` command.

```
user@host# show tenants TSYS1
security {
    log {
        report;
    }
}
```

NOTE: By default the `report` option is disabled.

Understanding On-Box and Off-Box Logging for Tenant System

SRX Series devices have two types of log: system logs and security logs. System logs record control plane events, for example admin login to the device. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy.

Starting in Junos OS Release 19.2R1, on-box logging configurations are supported for each tenant system and logs are handled based on these configurations.

The two types of log can be collected and saved either on-box or off-box.

Stream mode is a set of logging services that includes:

- Off-box logging (SRX Series)
- On-box logging (SRX1500, SRX4100, SRX4200, and SRX4600 Series)

Per tenant system configuration is supported for the off-box logging and logs are handled based on these configurations. The tenant system logs for off-box logging can only be generated from the tenant system interface.

Configure the security files in **binary/syslog/sd-syslog/welf** format for stream-mode and binary format for event-mode by using the log statement at the `[set tenants TSYS1 security]` hierarchy level.

NOTE: You cannot configure the security log file path for Tenant System.

For on-box logging with stream mode with binary format log, the `set security log stream` *`stream-name`* `file` command is configured per tenant system. The file name must be end with **.bin**. For example **TSYS1_f1.bin** in tenant system TSYS1. A new file **TSYS1_f1.bin** is created in the **/var/traffic-log/tenant-systems/** ***TSYS1*** directory.

For on-box logging with stream mode with other format logs, the `set security log stream` *`stream-name`* `file` command is configured per tenant system. For example tenant system TSYS1. A new file with the name configured is created in the **/var/traffic-log/tenant-systems/** ***TSYS1*** directory.

Configuring On-Box Binary Security Log Files for Tenant System

SRX Series devices support two types of log: system logs and security logs.

The two types of log are collected and saved either on-box or off-box. The following procedure explains how to configure security logs in binary format for on-box (event-mode and stream-mode) logging for tenant system.

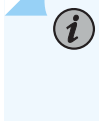
The following procedure specifies binary format for event-mode security logging, and defines the log filename, path, and log file characteristics for tenant system.

1. Specify the logging mode and the format for the log file. For on-box, event-mode logging:

```
[edit]
user@host# set tenants TSYS1 security log mode event
user@host# set tenants TSYS1 security log format binary
```

2. (Optional) Specify a log filename.

```
[edit]
user@host# set tenants TSYS1 security log file name security-binary-log
```



NOTE: Security log filename is not mandatory. If security log filename is not configured, by default the file bin_messages is created in the /var/log directory.

3. Confirm your configuration by entering the `show tenants TSYS1` command.

```
[edit]
user@host# show tenants TSYS1
security {
    log {
        mode event;
        format binary;
        file {
            name security-binary-log;
        }
    }
}
```

The following procedure specifies binary format for stream-mode security logging, and defines the log filename and log file characteristics for tenant system.

1. Specify the logging mode and the format for the log file. For on-box, stream-mode logging:

```
[edit]
user@host# set tenants TSYS1 security log mode stream
user@host# set tenants TSYS1 security log stream s1 format binary
```

2. (Optional) Specify a log filename.

```
[edit]
user@host# set tenants TSYS1 security log stream s1 file name f1.bin
```

3. Confirm your configuration by entering the `show tenants TSYS1` command.

```
[edit]
user@host# show tenants TSYS1
security {
    log {
        mode stream;
        stream s1 {
            format binary;
            file {
                name f1.bin;
            }
        }
    }
}
```

Configuring Off-Box Binary Security Log Files for Tenant System

SRX Series devices support two types of log: system logs and security logs.

The two types of log can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

The following procedure specifies binary format for stream-mode security logging, and defines the logging mode, source address, and host name characteristics for tenant system.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging:

```
[edit]
user@host# set tenants TSYS1 security log mode stream s1 format binary
```

2. Specify the source address for off-box security logging.

```
[edit]
user@host# set tenants TSYS1 security log source-address 100.0.0.1
```

3. Specify the host name.

```
[edit]
user@host# set tenants TSYS1 security log stream s1 host 100.0.0.2
```

4. Confirm your configuration by entering the `show tenants TSYS1` command.

```
[edit]
user@host# show tenants TSYS1
security {
    log {
        mode stream;
        source-address 100.0.0.1;
        stream s1 {
            format binary;
            host {
                100.0.0.2;
            }
        }
    }
}
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.2R1	Starting in Junos OS Release 19.2R1, on-box logging configurations are supported for each tenant system and logs are handled based on these configurations

AppQoS for Tenant Systems

IN THIS SECTION

Application quality of service (AppQoS) enable you to identify and control access to specific applications and provides the granularity of the stateful firewall rule base to match and enforce quality of service (QoS) at the application layer. AppQoS feature expands the capability of Junos OS class of service (CoS) for tenant systems.

Application Quality of Service for Tenant Systems Overview

The application quality of service (AppQoS) feature expands the capability of Junos OS class of service (CoS) for tenant systems. This includes marking DSCP values based on Layer-7 application types, honoring application-based traffic through loss priority settings, and controlling transfer rates on egress PICs based on Layer-7 application types.

When a network experiences congestion and delay, some packets must be dropped. Junos OS CoS allows you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to the rules you configure.

Tenant system enables you to partition a single device into multiple domains to perform security and routing functions.

Starting in Junos OS Release 19.3R1, AppQoS is supported when the SRX Series Firewall is configured with tenant system. You can configure a default AppQoS rule set to manage the application- traffic-control within the tenant system. AppQoS provides the ability to prioritize and meter the application traffic to provide better service to business-critical or high-priority application traffic.

AppQoS rule sets are included in the tenant system to implement application-aware quality-of-service control. You can configure a rule set with rules under the application-traffic-control option, and attach the AppQoS rule set to a tenant system as an application service. If the traffic matches the specified application the application-aware quality of service is applied for tenant system.

For AppQoS, traffic is grouped based on rules that associate a defined forwarding class with selected applications for tenant system. The match criteria for the rule includes one or more applications. When traffic from a matching application encounters the rule, the rule action sets the forwarding class, and remarks the DSCP value and loss priority to values appropriate for the application.

The AppQoS DSCP rewriter conveys a packet's quality of service through both the forwarding class and a loss priority. The AppQoS rate-limiting parameters control the transmission speed and volume for its associated queues for tenant system. The default AppQoS rule set is leveraged from one of the existing AppQoS rule sets, which are configured under the `[edit class-of-service application-traffic-control]` hierarchy level.

Rate limiters are applied in rules based on the application of the traffic for tenant system. Two rate limiters are applied for each session: `client-to-server` and `server-to-client`. This usage allows traffic in each direction to be provisioned separately.

Example: Configure Application Quality of Service for Tenant Systems

IN THIS SECTION

This example shows how to enable application quality of service (AppQoS) within a tenant system to provide prioritization and rate limiting for the traffic.

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall configured with tenant systems.
- Junos OS Release 19.3R1 and later releases.

Before you begin:

- Read the "Application Quality of Service for Tenant Systems Overview" on page 746 to understand how and where this procedure fits in the overall support for AppQos.

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

Overview

In this example, you configure an AppQoS rule set and invoke AppQoS as an application service in the tenant systems. You configure the class of service (CoS) for tenant systems. The AppQoS rule sets are included in the tenant systems to implement application-aware quality-of-service control.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set tenants TSYS1 class-of-service application-traffic-control rate-limiters HTTP-BW-RL
bandwidth-limit 512
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 match
application junos:HTTP
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 then
forwarding-class best-effort
```

```
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 then dscp-
code-point 001000
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 then loss-
priority high
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 then log
set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule RL1 then rate-
limit server-to-client HTTP-BW-RL
set tenants TSYS1 security policies from-zone untrust to-zone trust policy from_internet match
source-address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy from_internet match
destination-address any
set tenants TSYS1 security policies from-zone untrust to-zone trust policy from_internet match
application any
set tenants TSYS1 security policies from-zone trust to-zone trust policy p1 match dynamic-
application junos:web
set tenants TSYS1 security policies from-zone untrust to-zone trust policy from_internet then
permit application-services application-traffic-control rule-set RS1
```

Configuring AppQoS with a Tenant 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.

To configure AppQoS for a tenant system:

1. Configure the AppQoS real-time run information about application rate limiting of current or recent sessions for tenant system TSYS1.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rate-limiters HTTP-
BW-RL bandwidth-limit 512
```

2. Configure the AppQoS rules and application match criteria for tenant system TSYS1.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 match application junos:HTTP
```

3. Configure the AppQoS rules and the forwarding class for tenant system TSYS1.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 then forwarding-class best-effort
```

4. Configure the AppQoS rules and the dscp-code-point for tenant system TSYS1.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 then dscp-code-point 001000
```

5. Configure the AppQoS rules and the loss priority for tenant system TSYS1.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 then loss-priority high
```

6. Assign the rate limiters for rule-sets.

```
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 then log
user@host# set tenants TSYS1 class-of-service application-traffic-control rule-sets RS1 rule
RL1 then rate-limit server-to-client HTTP-BW-RL
```

7. Assign the class-of-service rule set to the security policy for tenant system TSYS1.

```
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy
from_internet match source-address any
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy
from_internet match destination-address any
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy
from_internet match application any
user@host# set tenants TSYS1 security policies from-zone trust to-zone trust policy p1 match
dynamic-application junos:web
user@host# set tenants TSYS1 security policies from-zone untrust to-zone trust policy
from_internet then permit application-services application-traffic-control rule-set RS1
```

Results

From configuration mode, confirm your configuration by entering the `show tenants TSYS1` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show tenants TSYS1
security {
    policies {
        from-zone untrust to-zone trust {
            policy from_internet {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            application-traffic-control {
                                rule-set RS1;
                            }
                        }
                    }
                }
            }
        }
        from-zone trust to-zone trust {
            policy p1 {
                match {
                    dynamic-application junos:web;
                }
            }
        }
    }
}
class-of-service {
    application-traffic-control {
        rate-limiters HTTP-BW-RL {
            bandwidth-limit 512;
        }
        rule-sets RS1 {
```

```
            rule RL1 {
                match {
                    application junos:HTTP;
                }
                then {
                    forwarding-class best-effort;
                    dscp-code-point 001000;
                    loss-priority high;
                    rate-limit {
                        server-to-client HTTP-BW-RL;
                    }
                    log;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

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

Verifying the class-of-service application-traffic-control counter

Purpose

Verify the class-of-service application-traffic-control counter for tenant systems.

Action

To verify the configuration is working properly, enter the `show class-of-service application-traffic-control counter tenant TSYS1` command.

```
user@host>show class-of-service application-traffic-control counter tenant TSYS1
Tenant System: TSYS1

pic: 0/0
  Counter type                                                Value
 Sessions processed                                           1
 Sessions marked                                              0
 Sessions honored                                             0
 Sessions rate limited                                        0
 Client-to-server flows rate limited                          0
 Server-to-client flows rate limited                          0
 Session default ruleset hit                                  0
 Session ignored no default ruleset                           0
```

Meaning

The output displays AppQoS DSCP marking and honoring statistics based on Layer 7 application classifiers.

Verifying the class-of-service application-traffic-control statistics rate-limiter

Purpose

Verify the class-of-service application-traffic-control statistics rate-limiter for tenant systems.

Action

To verify the configuration is working properly, enter the `show class-of-service application-traffic-control statistics rate-limiter tenant TSYS1` command.

```
user@host>show class-of-service application-traffic-control statistics rate-limiter tenant TSYS1
Tenant System: TSYS1

pic: 0/0
```

Meaning

The output displays AppQoS real-time run information about application rate limiting of current or recent sessions.

Application Security for Tenant Systems

IN THIS SECTION

Application Security in tenant systems identifies application traffic traversing your network regardless of port, protocol, and encryption, and thereby provides greater visibility to control network traffic. The application security controls network traffic by setting and enforcing security policies based on accurate application information.

Application Identification Services for Tenant Systems Overview

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

- 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 tenant systems, predefined and custom application signatures are global resources that are shared by all tenant systems. Application identification (AppID) is enabled by default for a tenant system. The following are the privileges and responsibilities of the primary administrator over AppID:

- Download and install the predefined Juniper Networks application signatures.

- Create custom application and nested application signatures to identify applications that are not a part of the predefined database.
- View or clear the application identification statistics and counters for all tenant systems.
- Uninstall application signature package.

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 tenant system has its own ASC. A tenant system or the primary administrator can view or clear ASC entries for any tenant system.

The AppID support for tenant systems include two options to view or clear tenant system statistics and tenant system counters for their own tenant system. Because the statistics reset time is common across the tenant systems, when you configure a new tenant system for the very first time, the statistics for that tenant system may get cleared even before the configured statistics reset time.

The custom signatures configured by the primary administrator can be configured in the tenant system security policies.

As a primary administrator or a tenant system user, you can use the commands `show services application-identification status` and `show services application-identification version` to view the status and version information about the AppID signature package.

4

CHAPTER

Configuration Statements and Operational Commands

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands