Engineering Simplicity

Junos® OS

Security Policies User Guide for Security Devices

Published
2026-01-05

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

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 security zones, address books and address sets, security policy applications and application sets, and security policies in Junos OS on the SRX Series Firewalls.

1

CHAPTER

Overview

IN THIS CHAPTER

Security Basics Overview

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

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

RELATED DOCUMENTATION

Getting Started Guide for Junos OS

Security Policies Overview

IN THIS SECTION

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

In a Junos OS stateful firewall, the security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. From the perspective of security policies, the traffic enters one security zone and exits another security zone. This combination of a *from-zone* and *to-zone* is called a *context*. Each context contains an *ordered list* of policies. Each policy is processed in the order that it is defined within a context.

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

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

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

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

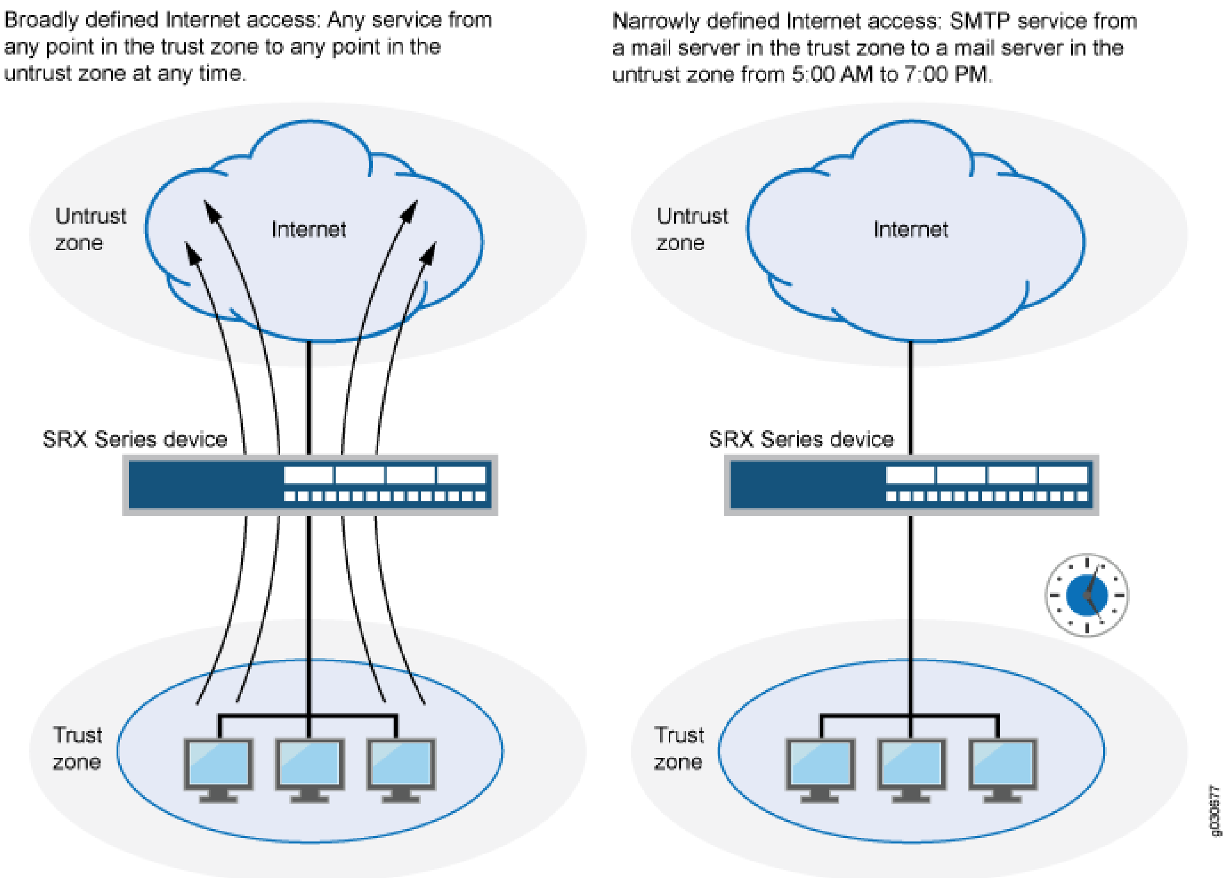
- To view logs from denied connections, enable log on `session-init`.
- To log sessions after their conclusion/tear-down, enable log on `session-close`.

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

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

At the broadest level, you can allow all kinds of traffic from any source in one zone to any destination in all other zones without any scheduling restrictions. At the narrowest level, you can create a policy that allows only one kind of traffic between a specified host in one zone and another specified host in another zone during a scheduled interval of time. See Figure 1 on page 4.

Figure 1: Security Policy



Every time a packet attempts to pass from one zone to another or between two interfaces bound to the same zone, the device checks for a policy that permits such traffic (see "Understanding Security Zones" on page 7 and "Example: Configuring Security Policy Applications and Application Sets" on page 56). To allow traffic to pass from one security zone to another—for example, from zone A to zone B—you must configure a policy that permits zone A to send traffic to zone B. To allow traffic to flow the other way, you must configure another policy permitting traffic from zone B to zone A.

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

Platform-Specific Security Policies Behavior

Use Feature Explorer to confirm platform and release support for specific features.

Use the following table to review platform-specific behavior for your platform:

<table>
<tr><th>Platform</th><th>Difference</th></tr>
<tr><td rowspan="2">SRX Series</td><td>SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices that support a factory-default security policy:
Allows all traffic from the trust zone to the untrust zone.
Allows all traffic between trusted zones, that is from the trust zone to intrazone trusted zones.
Denies all traffic from the untrust zone to the trust zone.</td></tr>
<tr><td>On SRX Series devices that support virtual systems, policies set in the root system do not affect policies set in virtual systems.</td></tr>
</table>

RELATED DOCUMENTATION

Configuring Security Policies | 96

2

CHAPTER

Security Zones

IN THIS CHAPTER

Security Zones

IN THIS SECTION

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

Security Zones Overview

IN THIS SECTION

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

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

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

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

From the perspective of security policies, traffic enters into one security zone and goes out on another security zone. This combination of a `from-zone` and a `to-zone` is defined as a *context*. Each context contains an ordered list of policies. For more information on policies, see "Security Policies Overview" on page 2.

This topic includes the following sections:

Understanding Security Zone Interfaces

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

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

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

Understanding Functional Zones

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

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

Understanding Security Zones

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

Security zones have the following properties:

- Policies—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall. For more information, see "Security Policies Overview" on page 2.

- Screens—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful. For more information, see Reconnaissance Deterrence Overview.

- Address books—IP addresses and address sets that make up an address book to identify its members so that you can apply policies to them. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and Domain Name System (DNS) names. For more information, see "Example: Configuring Address Books and Address Sets" on page 36.

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

- Interfaces—List of interfaces in the zone.

Security zones have the following preconfigured zone:

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

Example: Creating Security Zones

IN THIS SECTION

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

Requirements

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

Overview

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

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

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

Step-by-Step Procedure

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

To create zones and assign interfaces to them:

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

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

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

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

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

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

Results

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

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

```
[edit]

user@host# show security zones security-zone ABC
...
    interfaces {
        ge-0/0/1.0 {
            ...
        }
    }
```

```
[edit]

user@host# show interfaces ge-0/0/1
...
        unit 0 {
        family inet {
            address 203.0.113.1/24;
        }
        family inet6 {
            address 2001:db8:1::1/64;
        }
    }
```

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

Verification

IN THIS SECTION

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

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

Supported System Services for Host Inbound Traffic

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

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

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

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

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

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

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

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

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

Understanding How to Control Inbound Traffic Based on Traffic Types

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

Note the following:

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

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

Example: Controlling Inbound Traffic Based on Traffic Types

IN THIS SECTION

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

Requirements

Before you begin:

- Configure network interfaces. See Interfaces User Guide for Security Devices.
- Understand Inbound traffic types. See "Understanding How to Control Inbound Traffic Based on Traffic Types" on page 13.

Overview

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

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

Configuration

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

Step-by-Step Procedure

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

To configure inbound traffic based on traffic types:

1. Configure a security zone.

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

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

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

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

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

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

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

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

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

Results

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

```
[edit]

user@host# show security zones security-zone ABC
host-inbound-traffic {
    system-services {
        all;
    }
}
    interfaces {
    ge-0/0/1.3 {
        host-inbound-traffic {
            system-services {
                ftp;
                telnet;
                snmp;
            }
        }
    }
    ge-0/0/1.0 {
        host-inbound-traffic {
            system-services {
                all;
                ftp {
                    except;
                }
                http {
                    except;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

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

Understanding How to Control Inbound Traffic Based on Protocols

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

Any host-inbound traffic that corresponds to a protocol listed under the host-inbound traffic option is allowed. For example, if anywhere in the configuration, you map a protocol to a port number other than the default, you can specify the protocol in the host-inbound traffic option, and the new port number will be used. Table 1 on page 18 lists the supported protocols. A value of `all` indicates that traffic from all of the following protocols is allowed inbound on the specified interfaces (of the zone, or a single specified interface).

Table 1: Supported Inbound System Protocols

Supported System Services			
all	igmp	pim	sap
bfd	ldp	rip	vrrp

Table 1: Supported Inbound System Protocols *(Continued)*

Supported System Services			
bgp	msdp	ripng	nhrp
router-discovery	dvmrp	ospf	rsvp
pgm	ospf3		

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

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

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

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

Example: Controlling Inbound Traffic Based on Protocols

IN THIS SECTION

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

Requirements

Before you begin:

- Configure security zones. See "Example: Creating Security Zones" on page 9.
- Configure network interfaces. See the Interfaces User Guide for Security Devices.

Overview

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

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

Configuration

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

Step-by-Step Procedure

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

To configure inbound traffic based on protocols:

1. Configure a security zone.

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

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

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

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

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

Results

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

```
[edit]
user@host# show security zones security-zone ABC
interfaces {
    ge-0/0/1.0 {
        host-inbound-traffic {
            protocols {
                ospf;
                ospf3;
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

Troubleshooting with Logs

Purpose

Use these logs to identify any issues.

Action

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

Example: Configuring the TCP-Reset Parameter

IN THIS SECTION

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

Requirements

Before you begin, configure security zones. See "Example: Creating Security Zones" on page 9.

Overview

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

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

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

To configure the TCP-Reset parameter for a zone:

1. Configure a security zone.

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

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

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

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

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

Verification

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

Platform-Specific Security Zones Creation Behavior

Use Feature Explorer to confirm platform and release support for specific features.

Use the following table to review platform-specific behavior for your platform:

Platform	Difference
SRX Series	• On SRX3400, SRX3600, SRX4600, SRX4700, and SRX5400 devices, you can configure 2000 interfaces within a security zone, depending on the Junos OS release in your installation.

RELATED DOCUMENTATION

Configuring Security Policies | 96

3

CHAPTER

Address Books and Address Sets

IN THIS CHAPTER

Address Books and Address Sets

IN THIS SECTION

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

An address book within a zone can consist of individual addresses or address sets. An address set is a set of one or more addresses defined within an address book. Using address sets, you can organize addresses in logical groups. Address sets are useful when you must refer to a group of addresses more than once in a security policy, in a security zone, or NAT configuration.

Understanding Address Books

IN THIS SECTION

An address book is a collection of addresses and address sets. Junos OS allows you to configure multiple address books. You can add addresses to address books or use the predefined addresses available to each address book by default.

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

Predefined Addresses

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

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

Network Prefixes in Address Books

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

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

Wildcard Addresses in Address Books

Besides IP addresses and domain names, you can specify a wildcard address in an address book. A wildcard address is represented as A.B.C.D/wildcard-mask. The wildcard mask determines which of the bits in the IP address A.B.C.D should be ignored. For example, the source IP address 192.168.0.11/255.255.0.255 in a security policy implies that the security policy match criteria can discard the third octet in the IP address (symbolically represented as 192.168.*.11). Therefore, packets with source IP addresses such as 192.168.1.11 and 192.168.22.11 conform to the match criteria. However, packets with source IP addresses such as 192.168.0.1 and 192.168.1.21 do not satisfy the match criteria.

The wildcard address usage is not restricted to full octets only. You can configure any wildcard address. For example, the wildcard address 192.168.7.1/255.255.7.255 implies that you need to ignore only the first 5 bits of the third octet of the wildcard address while making the policy match. If the wildcard address usage is restricted to full octets only, then wildcard masks with either 0 or 255 in each of the four octets only will be permitted.

DNS Names in Address Books

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

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

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

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

```
user@host# set system name-server 10.5.0.1 source-address 10.4.0.1
```

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

Understanding Global Address Books

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

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

Global address books are used in the following cases:

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

Understanding Address Sets

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

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

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

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

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

Configuring Addresses and Address Sets

IN THIS SECTION

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

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

Addresses and Address Sets

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

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

```
[edit security address-book book1]
user@host# set address a1 203.0.113.1
user@host# set address a2 203.0.113.4/30
user@host# set address a4 2001:db8::/32
user@host# set address a5 2001:db8:1::1/127
user@host# set address example dns-name www.example.com
user@host# set address-set set1 address a1
user@host# set address-set set1 address a2
user@host# set address-set set1 address a2
user@host# set address-set set2 address bbc
```

When defining addresses and address sets, follow these guidelines:

- Address sets can only contain address names that belong to the same security zone.

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

Address Books and Security Zones

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

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

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

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

Address Books and Security Policies

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

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

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

Addresses Available for Security Policies

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

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

For example, suppose you configure addresses in two address books—`global` and `book1`. Then, display the addresses that you can configure as source or destination addresses in a policy (see Table 2 on page 32).

Table 2: Available Addresses Displayed in the CLI

<table>
<tr><th>Addresses Configured</th><th>Addresses Displayed in the CLI</th></tr>
<tr><td><pre>[edit security address-book]
set global address a1 203.0.113.0/24;
set global address a2 198.51.100.0/24;
set global address a3 192.0.2.0/24;
set book1 address a1 203.0.113.128/25;</pre></td><td><pre>[edit security policies from-zone trust to-zone untrust]
user@host# set policy p1 match set match source-address ?

Possible completions:
  [Open a set of values
  a1   The address in address book book1
  a2   The address in address book global
  a3   The address in address book global
  any   Any IPv4 or IPv6 address
  any-ipv4   Any IPv4 address
  any-ipv6   Any IPv6 address</pre></td></tr>
</table>

The addresses displayed in this example illustrate:

- Addresses in a user-defined address book have a higher lookup priority than addresses in the global address book.
- Addresses in a global address book have a higher priority than the predefined addresses `any`, `any-ipv4`, and `any-ipv6`.

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

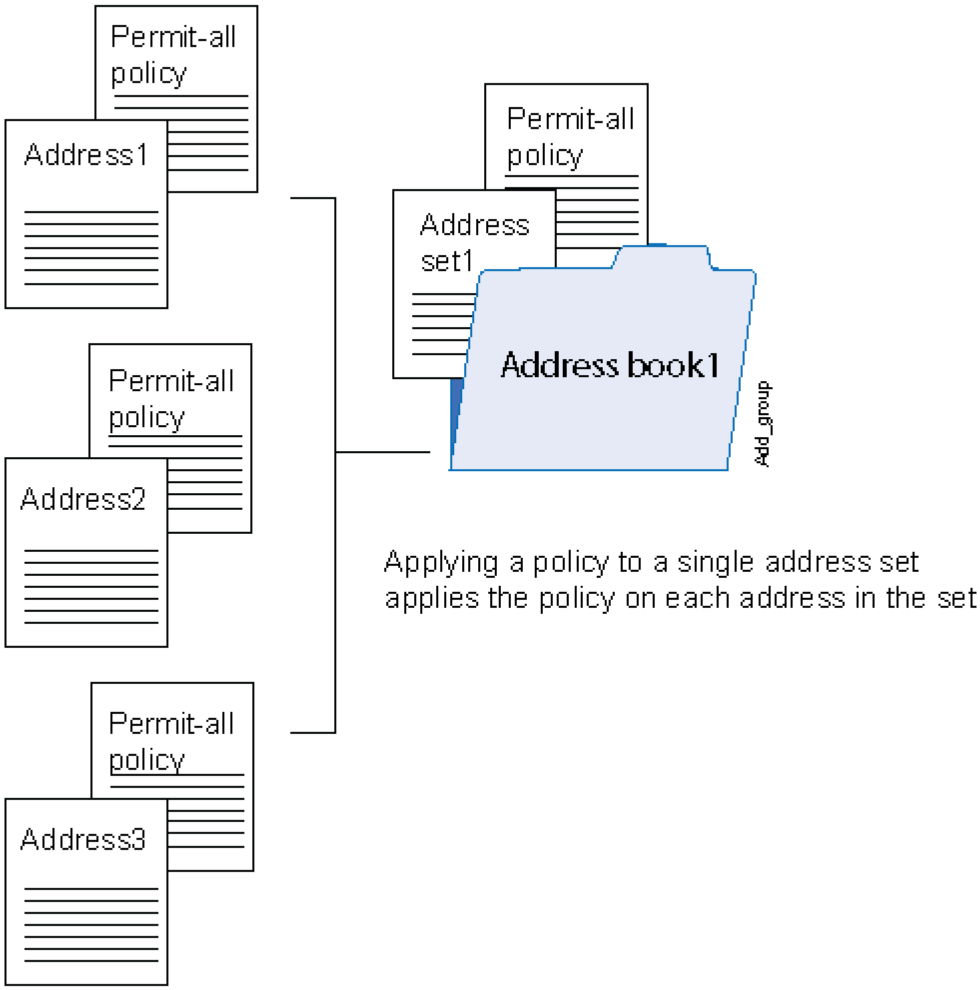
Applying Policies to Address Sets

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

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

Figure 2 on page 34 shows how policies are applied to address sets.

Figure 2: Applying Policies to Address Sets



Using Addresses and Address Sets in NAT Configuration

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

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

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

When configuring address books with NAT, follow these guidelines:

- In a NAT rule, you can specify addresses from a global address book only. User-defined address books are not supported with NAT.
- You can configure an address set as a source address name in a source NAT rule. However, you cannot configure an address set as a destination address name in a destination NAT rule.

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

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

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

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

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

Example: Configuring Address Books and Address Sets

IN THIS SECTION

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

Requirements

Before you begin:

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

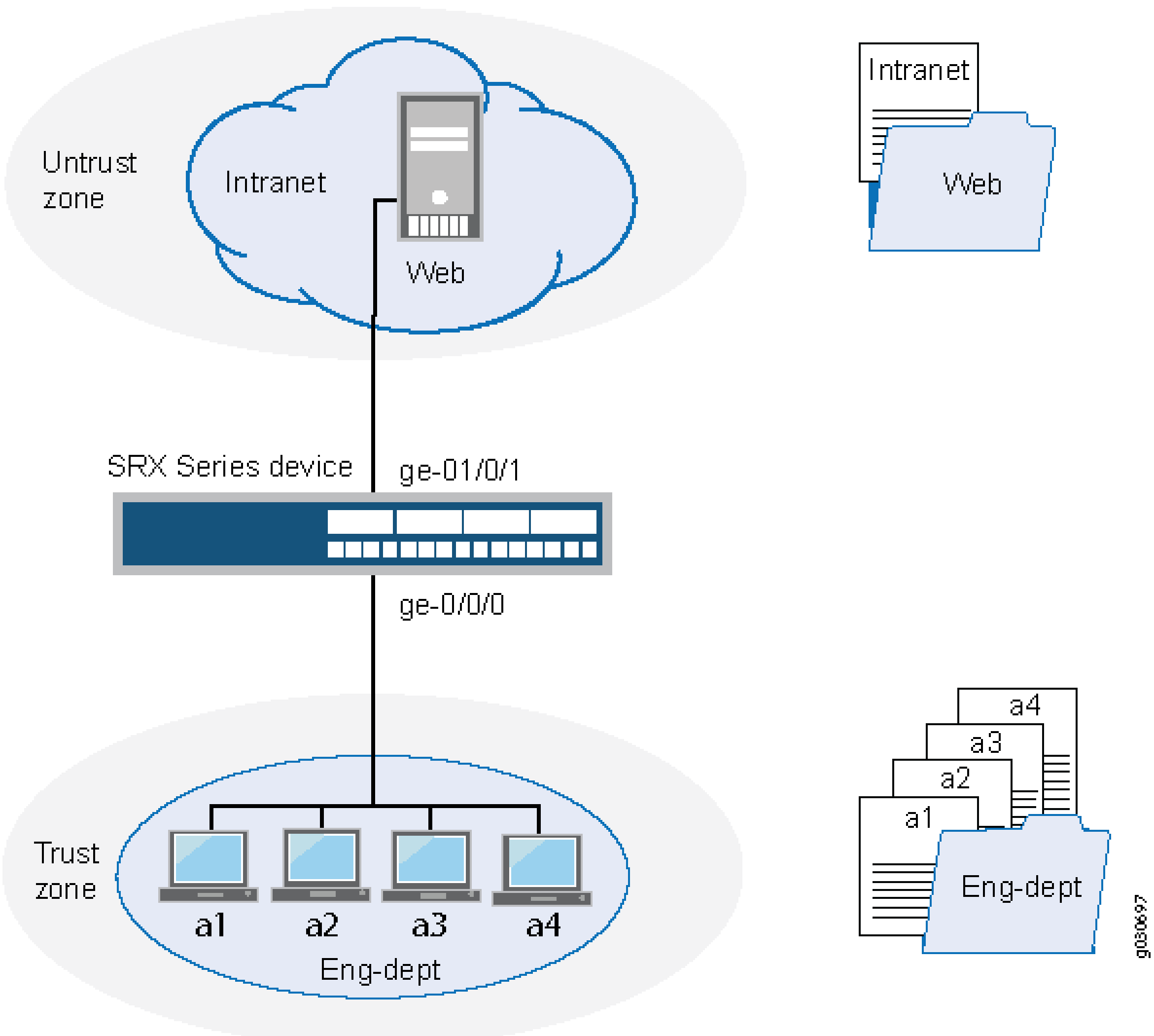
Overview

IN THIS SECTION

In this example, you configure an address book with addresses and address sets (see Figure 3 on page 37) to simplify configuring your company's network. You create an address book called `Eng-dept` and add addresses of members from the Engineering department. You create another address book called `Web` and add a DNS name to it. Then you attach a security zone trust to the `Eng-dept` address book and security zone untrust to the `Web` address book. You also create address sets to group software and hardware addresses in the Engineering department. You plan to use these addresses as source address and destination addresses in your future policy configurations.

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

Figure 3: Configuring Addresses and Address Sets



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 interfaces ge-0/0/0 unit 0 family inet address 203.0.113.5

set interfaces ge-0/0/1 unit 0 family inet address 203.0.113.6

set security zones security-zone trust interfaces ge-0/0/0

set security zones security-zone untrust interfaces ge-0/0/1

set security address-book Eng-dept address a1 203.0.113.1

set security address-book Eng-dept address a2 203.0.113.2

set security address-book Eng-dept address a3 203.0.113.3

set security address-book Eng-dept address a4 203.0.113.4
```

```
set security address-book Eng-dept address-set sw-eng address a1

set security address-book Eng-dept address-set sw-eng address a2

set security address-book Eng-dept address-set hw-eng address a3

set security address-book Eng-dept address-set hw-eng address a4

set security address-book Eng-dept attach zone trust

set security address-book Web address Intranet dns-name www-
int.device1.example.com

set security address-book Web attach zone untrust

set security address-book global address g1 198.51.100.2
```

Step-by-Step Procedure

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

To configure addresses and address sets:

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

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

2. Create security zones and assign interfaces to them.

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

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

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

4. Create address sets.

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

5. Attach the address book to a security zone.

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

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

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

7. Define an address in the global address book.

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

Results

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

```
[edit]
user@host# show security zones
    security-zone trust {

        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/1.0;
        }
    }
```

```
[edit]
user@host# show security address-book
        Eng-dept {
            address a1 203.0.113.1/32;
            address a2 203.0.113.2/32;
            address a3 203.0.113.3/32;
            address a4 203.0.113.4/32;
            address-set sw-eng {
                address a1;
                address a2;
            }
            address-set hw-eng {
                address a3;
                address a4;
            }
            attach {
                zone trust;
            }
        }
            Web {
                address Intranet {
                    dns-name www-int.device1.example.com;
                }
                attach {
                    zone untrust;
                }
            }
            global {
                address g1 198.51.100.2/32;
            }
```

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying Address Book Configuration

Purpose

Display information about configured address books and addresses.

Action

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

```
user@host#
show security address-book
Eng-dept {
    address a1 203.0.113.1/32;
    address a2 203.0.113.2/32;
    address a3 203.0.113.3/32;
    address a4 203.0.113.4/32;
    address-set sw-eng {
        address a1;
        address a2;
    }
    address-set hw-eng {
        address a3;
        address a4;
    }
    attach {
        zone trust;
    }
}
Web {
    address Intranet {
        dns-name www-int.device1.example.com;
    }
    attach {
        zone untrust;
    }
}
```

```
global {
    address g1 198.51.100.2/32;
}
```

Verifying Global Address Book Configuration

Purpose

Display information about configured addresses in the global address book.

Action

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

```
user@host#
show security address-book global
address g1 198.51.100.2/32;
```

Excluding Addresses from Policies

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

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

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

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

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

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

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

Example: Excluding Addresses from Policies

IN THIS SECTION

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

Requirements

This example uses the following hardware and software components:

- An SRX Firewall
- A PC
- Any supported Junos OS Release

Before you begin, configure address books and address sets. See "Example: Configuring Address Books and Address Sets" on page 36.

Overview

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

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

Configuration

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

Step-by-Step Procedure

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

To configure negated addresses:

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

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

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

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

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

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

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

```
[edit security address book ]
user@host#set DES-ADDR address ad8 198.51.100.1/24
user@host#set DES-ADDR address ad9 range-address 192.0.2.117 to 192.0.2.199
user@host#set DES-ADDR address ad10 198.51.100.0/24
user@host#set DES-ADDR address ad11 range-address 192.0.2.199 to 192.0.2.250
```

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

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

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

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

7. Specify the policy name and source address.

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

8. Exclude source addresses from the policy.

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

9. Specify the destination address.

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

10. Exclude destination addresses from the policy.

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

11. Configure the security policy application.

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

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

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

Results

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

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

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying the Policy Configuration

Purpose

Verify that the policy configuration is correct.

Action

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

```
user@host>show security policies policy-name p1
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit
```

This output summarizes the policy configuration.

Verifying the Policy Configuration Detail

Purpose

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

Action

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

```
user@host>show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
    ad1(SOU-ADDR): 255.255.255.255/32
    ad2(SOU-ADDR): 203.0.113.130/25
```

```
    ad3(SOU-ADDR): 192.0.2.6 ~ 192.0.2.116
    ad4(SOU-ADDR): 192.0.2.128/25
    Destination addresses(excluded):
    ad8(DES-ADDR): 198.51.100.1/24
    ad9(DES-ADDR): 192.0.2.117 ~ 192.0.2.199
    ad10(DES-ADDR): 198.51.100.0/24
    ad11(DES-ADDR): 192.0.2.199 to 192.0.2.250
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

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

SEE ALSO

Predefined Policy Applications | 62
Custom Policy Applications | 85

Platform-Specific Policies, Address Books and Address Sets Behavior

IN THIS SECTION

Platform-Specific DNS Names in Address Books Behavior

Use Address books and Feature Explorer to confirm platform and release support for specific features.

Use the following table to review platform-specific behavior for your platform:

Platform	Difference
SRX Firewalls and vSRX3.0	• For SRX5400 devices and vSRX3.0 Virtual Firewall instances, management traffic can originate from a specific source address for Domain Name System (DNS) names.

Platform-Specific Addresses and Address Sets Behavior

Platform	Difference Address Objects Per Security Policy
SRX Firewalls	• On SRX Firewalls that support addresses and address sets, one policy can reference multiple address sets, multiple address entries, or both. One address set can reference a maximum of 16384 address entries and a maximum of 256 address sets. • On SRX Firewalls that support addresses and address sets, every IPv6 address entry is equal to one address object per policy. Example: To configure an SRX345 device which has a limitation of 2048 address objects per policy, you can configure 2040 IPv4 entries and 8 IPv6 entries (2040 + 8 = 2048) and commit the configuration. When you configure 2040 IPv4 address entries and 9 IPv6 address entries (2040+9 = 2049), you'll get the following error message when you attempt to commit the configuration: `"Error exceeding maximum limit of source addresses per policy (2048)"` There is a limit to the number of address objects that a policy can reference; the maximum number of address objects per policy is different for different platforms as shown in table below. See Best Practices for Defining Policies on SRX Firewalls for details on the maximum number of policies per context for SRX Firewalls.
	SRX5400 devices support a maximum of 16,000 address objects per policy and a maximum of 80,000 policies per context.

4

CHAPTER

Security Policy Applications and Application Sets

IN THIS CHAPTER

Security Policy Applications and Application Sets

IN THIS SECTION

Policy applications are types of traffic for which protocol standards exist. The policy application set is a group of policy applications. Junos OS simplifies the process by allowing you to manage a small number of policy application sets, rather than a large number of individual policy application entries.

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

Security Policy Applications Overview

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

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

NOTE: Each predefined application has a source port range of `1-65535`, which includes the entire set of valid port numbers. This prevents potential attackers from gaining access by using a source port outside of the range. If you need to use a different source port range for any predefined application, create a custom application. For information, see "Understanding Custom Policy Applications" on page 86.

SEE ALSO

Understanding Security Policy Elements | 96

Security Policy Application Sets Overview

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

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

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

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

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

Example: Configuring Security Policy Applications and Application Sets

IN THIS SECTION

This example shows how to configure applications and application sets.

Requirements

Before you begin, configure the required applications. See "Security Policy Application Sets Overview" on page 56.

Overview

IN THIS SECTION

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

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

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

Topology

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure an application and application set:

1. Create an application set for managers.

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

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

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

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

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

Verification

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

Understanding Policy Application Timeout Configuration and Lookup

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

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

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

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

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

2. The protocol-based default timeout table is searched for a timeout value. See Table 3 on page 59.

Table 3: Protocol-Based Default Timeout

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

Understanding Policy Application Timeouts Contingencies

When setting timeouts, be aware of the following contingencies:

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

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

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

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

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

Example: Setting a Policy Application Timeout

IN THIS SECTION

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

Requirements

Before you begin, understand policy application timeouts. See "Understanding Policy Application Timeout Configuration and Lookup" on page 59.

Overview

Application timeout values are stored in the application entry database and in the corresponding vsys TCP and UDP port-based timeout tables. In this example, you set the device for a policy application timeout to 75 minutes (4500 seconds) for the FTP predefined application.

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

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To set a policy application timeout:

1. Set the inactivity timeout value.

```
[edit applications application ftp]
user@host# set inactivity-timeout 4500
```

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

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

Verification

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

RELATED DOCUMENTATION

Custom Policy Applications | 85

Predefined Policy Applications

IN THIS SECTION

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

Understanding Internet-Related Predefined Policy Applications

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

Table 4 on page 63 lists Internet-related predefined applications. Depending on your network requirements, you can choose to permit or deny any or all of these applications. Each entry lists the application name, default receiving port, and application description.

Table 4: Predefined Applications

Application Name	Port(s)	Application Description
AOL	5190-5193	America Online Internet service provider (ISP) provides Internet, chat, and instant messaging applications.
DHCP relay	67 (default)	Dynamic Host Configuration Protocol.
DHCP	68 client 67 server	Dynamic Host Configuration Protocol allocates network addresses and delivers configuration parameters from server to hosts.
DNS	53	Domain Name System translates domain names into IP addresses.
FTP	20 data 21 control	File Transfer Protocol (FTP) allows the sending and receiving of files between machines. You can choose to deny or permit ANY or to selectively permit or deny. We recommend denying FTP applications from untrusted sources (Internet).
Gopher	70	Gopher organizes and displays Internet servers' contents as a hierarchically structured list of files. We recommend denying Gopher access to avoid exposing your network structure.

Table 4: Predefined Applications *(Continued)*

Application Name	Port(s)	Application Description
HTTP	80	HyperText Transfer Protocol is the underlying protocol used by the World Wide Web (WWW). Denying HTTP application disables your users from viewing the Internet. Permitting HTTP application allows your trusted hosts to view the Internet.
HTTP-EXT	–	Hypertext Transfer Protocol with extended nonstandard ports
HTTPS	443	Hypertext Transfer Protocol with Secure Sockets Layer (SSL) is a protocol for transmitting private documents through the Internet. Denying HTTPS disables your users from shopping on the Internet and from accessing certain online resources that require secure password exchange. Permitting HTTPS allows your trusted hosts to participate in password exchange, shop online, and visit various protected online resources that require user login.
Internet Locator Service	–	Internet Locator Service includes LDAP, User Locator Service, and LDAP over TSL/SSL.
IRC	6665-6669	Internet Relay Chat (IRC) allows people connected to the Internet to join live discussions.
LDAP	389	Lightweight Directory Access Protocol is a set of protocols used to access information directories.
PC-Anywhere	–	PC-Anywhere is a remote control and file transfer software.
TFTP	69	Trivial File transfer Protocol (TFTP) is a protocol for simple file transfer.

Table 4: Predefined Applications *(Continued)*

Application Name	Port(s)	Application Description
WAIS	—	Wide Area Information Server is a program that finds documents on the Internet.

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

Understanding Microsoft Predefined Policy Applications

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

Table 5 on page 65 lists predefined Microsoft applications, parameters associated with each application, and a brief description of each application. Parameters include universal unique identifiers (UUIDs) and TCP/UDP source and destination ports. A UUID is a 128-bit unique number generated from a hardware address, a timestamp, and seed values.

Table 5: Predefined Microsoft Applications

Application	Parameter/UUID	Description
Junos MS-RPC-EPM	135 e1af8308-5d1f-11c9-91a4-08002b14a0fa	Microsoft remote procedure call (RPC) Endpoint Mapper (EPM) Protocol.
Junos MS-RPC	—	Any Microsoft remote procedure call (RPC) applications.

Table 5: Predefined Microsoft Applications *(Continued)*

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

Table 5: Predefined Microsoft Applications *(Continued)*

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

Understanding Dynamic Routing Protocols Predefined Policy Applications

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

Depending on your network requirements, you can choose to permit or deny messages generated from these dynamic routing protocols and packets of these dynamic routing protocols. Table 6 on page 67 lists each supported dynamic routing protocol by name, port, and description.

Table 6: Dynamic Routing Protocols

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

Understanding Streaming Video Predefined Policy Applications

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

Table 7 on page 68 lists each supported streaming video application by name and includes the default port and description. Depending on your network requirements, you can choose to permit or deny any or all of these applications.

Table 7: Supported Streaming Video Applications

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

Understanding Sun RPC Predefined Policy Applications

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

Table 8 on page 69 lists each Sun remote procedure call Application Layer Gateway (RPC ALG) application name, parameters, and full name.

Table 8: RPC ALG Applications

Application	Program Numbers	Full Name
SUN-RPC-PORTMAPPER	111100000	Sun RPC Portmapper protocol
SUN-RPC-ANY	ANY	Any Sun RPC applications
SUN-RPC-PROGRAM-MOUNTD	100005	Sun RPC Mount Daemon
SUN-RPC-PROGRAM-NFS	100003 100227	Sun RPC Network File System
SUN-RPC-PROGRAM-NLOCKMGR	100021	Sun RPC Network Lock Manager
SUN-RPC-PROGRAM-RQUOTAD	100011	Sun RPC Remote Quota Daemon
SUN-RPC-PROGRAM-RSTATD	100001	Sun RPC Remote Status Daemon
SUN-RPC-PROGRAM-RUSERD	100002	Sun RPC Remote User Daemon
SUN-RPC-PROGRAM-SADMIND	100232	Sun RPC System Administration Daemon
SUN-RPC-PROGRAM-SPRAYD	100012	Sun RPC Spray Daemon
SUN-RPC-PROGRAM-STATUS	100024	Sun RPC Status
SUN-RPC-PROGRAM-WALLD	100008	Sun RPC Wall Daemon

Table 8: RPC ALG Applications *(Continued)*

Application	Program Numbers	Full Name
SUN-RPC-PROGRAM-YPBIND	100007	SUN RPC Yellow Page Bind application

Understanding Security and Tunnel Predefined Policy Applications

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

Table 9 on page 70 lists each supported application and gives the default port(s) and a description of each entry.

Table 9: Supported Applications

Application	Port	Description
IKE	UDP source 1-65535; UDP destination 500	Internet Key Exchange is the protocol that sets up a security association in the IPsec protocol suite. Internet Key protocol (IKE) is a protocol to obtain authenticated keying material for use with ISAKMP.
IKE-NAT	4500	IKE-Network Address Translation (NAT) performs Layer 3 NAT for S2C IKE traffic.
L2TP	1701	L2TP combines PPTP with Layer 2 Forwarding (L2F) for remote access.
PPTP	1723	Point-to-Point Tunneling Protocol allows corporations to extend their own private network through private *tunnels* over the public Internet.

Understanding IP-Related Predefined Policy Applications

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

Table 10 on page 71 lists the predefined IP-related applications. Each entry includes the default port and a description of the application.

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

Table 10: Predefined IP-Related Applications

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

Understanding Instant Messaging Predefined Policy Applications

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

Table 11 on page 71 lists predefined Internet-messaging applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 11: Predefined Internet-Messaging Applications

Application	Port	Description
Gnutella	6346 (default)	Gnutella is a public domain file sharing protocol that operates over a distributed network. You can assign any port, but the default is 6346.
MSN	1863	Microsoft Network Messenger is a utility that allows you to send instant messages and talk online.

Table 11: Predefined Internet-Messaging Applications *(Continued)*

Application	Port	Description
NNTP	119	Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages.
SMB	445	Server Message Block (SMB) over IP is a protocol that allows you to read and write files to a server on a network.
YMSG	5010	Yahoo! Messenger is a utility that allows you to check when others are online, send instant messages, and talk online.

Understanding Management Predefined Policy Applications

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

Table 12 on page 72 lists the predefined management applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 12: Predefined Management Applications

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

Table 12: Predefined Management Applications *(Continued)*

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

Table 12: Predefined Management Applications *(Continued)*

Application	Port	Description
Talk	517-518	Talk is a visual communication program that copies lines from your terminal to that of another user.
Telnet	23	Telnet is a UNIX program that provides a standard method of interfacing terminal devices and terminal-oriented processes to each other.
WinFrame	—	WinFrame is a technology that allows users on non-Windows machines to run Windows applications.
X-Windows	—	X-Windows is the windowing and graphics system that Motif and OpenLook are based on.

Understanding Mail Predefined Policy Applications

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

Table 13 on page 74 lists the predefined mail applications. Each includes the name of the application, the default or assigned port number, and a description of the application.

Table 13: Predefined Mail Applications

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

Understanding UNIX Predefined Policy Applications

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

Table 14 on page 75 lists the predefined UNIX applications. Each entry includes the name of the application, the default or assigned port, and a description of the application.

Table 14: Predefined UNIX Applications

Application	Port	Description
FINGER	79	Finger is a UNIX program that provides information about the users.
UUCP	117	UNIX-to-UNIX Copy Protocol (UUCP) is a UNIX utility that enables file transfers between two computers over a direct serial or modem connection.

Understanding Miscellaneous Predefined Policy Applications

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

Table 15 on page 75 lists predefined miscellaneous applications. Each entry includes the application name, default or assigned port, and a description of the application.

Table 15: Predefined Miscellaneous Applications

Application	Port	Description
CHARGEN	19	Character Generator Protocol is a UDP- or TCP-based debugging and measurement tool.
DISCARD	9	Discard protocol is an Application Layer protocol that describes a process for discarding TCP or UDP data sent to port 9.
IDENT	113	Identification protocol is a TCP/IP Application Layer protocol used for TCP client authentication.

Table 15: Predefined Miscellaneous Applications *(Continued)*

Application	Port	Description
LPR	515 listen; 721-731 source range (inclusive)	Line Printer Daemon protocol is a TCP-based protocol used for printing applications.
RADIUS	1812	Remote Authentication Dial-In User Service application is a server program used for authentication and accounting purposes.
RADIUS Accounting	1813	A RADIUS Accounting server receives statistical data about users logging in to or out of a LAN.
SQLMON	1434 (SQL Monitor Port)	SQL monitor (Microsoft)
VNC	5800	Virtual Network Computing facilitates viewing and interacting with another computer or mobile Juniper Networks device connected to the Internet.
WHOIS	43	Network Directory Application Protocol is a way to look up domain names.
SCCP	2000	Cisco Station Call Control Protocol (SCCP) uses the signaling connection control port to provide high availability and flow control.

Understanding ICMP Predefined Policy Applications

IN THIS SECTION

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

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

You can choose to permit or deny any or specific types of ICMP messages to improve network security. Some types of ICMP messages can be exploited to gain information about your network that might compromise security. For example, ICMP, TCP, or UDP packets can be constructed to return ICMP error messages that contain information about a network, such as its topology, and access list filtering characteristics. Table 16 on page 77 lists ICMP message names, the corresponding code, type, and description.

Table 16: ICMP Messages

ICMP Message Name	Type	Code	Description
ICMP-ANY	all	all	ICMP-ANY affects any protocol using ICMP. Denying ICMP-ANY impairs any attempt to ping or monitor a network using ICMP. Permitting ICMP-ANY allows all ICMP messages.
ICMP-ADDRESS-MASK • Request • Reply	17 18	0 0	ICMP address mask query is used for systems that need the local subnet mask from a bootstrap server. Denying ICMP address mask request messages can adversely affect diskless systems. Permitting ICMP address mask request messages might allow others to fingerprint the operating system of a host in your network.

Table 16: ICMP Messages *(Continued)*

ICMP Message Name	Type	Code	Description
ICMP-DEST-UNREACH	3	0	ICMP destination unreachable error message indicates that the destination host is configured to reject the packets. Codes 0, 1, 4, or 5 can be from a gateway. Codes 2 or 3 can be from a host (RFC 792). Denying ICMP destination unreachable error messages can remove the assumption that a host is up and running behind an SRX Series Firewall. Permitting ICMP destination unreachable error messages can allow some assumptions, such as security filtering, to be made about the network.
ICMP Fragment Needed	3	4	ICMP fragmentation error message indicates that fragmentation is needed but the don't fragment flag is set. We recommend denying these messages from the Internet to an internal network.
ICMP FragmentReassembly	11	1	ICMP fragment reassembly time exceeded error indicates that a host reassembling a fragmented message ran out of time and dropped the packet. This message is sometimes sent. We recommend denying these messages from the Internet (external) to the trusted (internal) network.

Table 16: ICMP Messages *(Continued)*

ICMP Message Name	Type	Code	Description
ICMP-HOST-UNREACH	3	1	ICMP host unreachable error messages indicate that routing table entries do not list or list as infinity a particular host. Sometimes this error is sent by gateways that cannot fragment when a packet requiring fragmentation is received. We recommend denying these messages from the Internet to a trusted network. Permitting these messages allows others to be able to determine your internal hosts IP addresses by a process of elimination or make assumptions about gateways and fragmentation.
ICMP-INFO • Request • Reply	15 16	0 0	ICMP-INFO query messages allow diskless host systems to query the network and self-configure. Denying ICMP address mask request messages can adversely affect diskless systems. Permitting ICMP address mask request messages might allow others to broadcast information queries to a network segment to determine computer type.
ICMP-PARAMETER-PROBLEM	12	0	ICMP parameter problem error messages notify you when incorrect header parameters are present and have caused a packet to be discarded We recommend denying these messages from the Internet to a trusted network. Permitting ICMP parameter problem error messages allows others to make assumptions about your network.

Table 16: ICMP Messages *(Continued)*

ICMP Message Name	Type	Code	Description
ICMP-PORT-UNREACH	3	3	ICMP port unreachable error messages indicate that gateways processing datagrams requesting certain ports are unavailable or unsupported in the network. We recommend denying these messages from the Internet to a trusted network. Permitting ICMP port unreachable error messages can allow others to determine which ports you use for certain protocols.
ICMP-PROTOCOL-UNREACH	3	2	ICMP protocol unreachable error messages indicate that gateways processing datagrams requesting certain protocols are unavailable or unsupported in the network. We recommend denying these messages from the Internet to a trusted network. Permitting ICMP protocol unreachable error messages can allow others to determine what protocols your network is running.
ICMP-REDIRECT	5	0	ICMP redirect network error messages are sent by an SRX Series Firewall. We recommend denying these messages from the Internet to a trusted network.
ICMP-REDIRECT-HOST	5	1	ICMP redirect messages indicate datagrams destined for the specified host to be sent along another path.
ICMP-REDIRECT-TOS-HOST	5	3	ICMP redirect type of service (TOS) and host error is a type of message.

Table 16: ICMP Messages *(Continued)*

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

Table 16: ICMP Messages *(Continued)*

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

Default Behavior of ICMP Unreachable Errors

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

- Sessions are closed for ICMP type-3, code-0, code-1, code-2, and code-3 messages only when the following conditions are met:

  - The ICMP unreachable message is received in the server–to-client direction.
  - No normal packet is received in the server-to-client direction.

  Otherwise, sessions do not close.

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

Example: Defining a Custom ICMP Application

IN THIS SECTION

This example shows how to define a custom ICMP application.

Requirements

Before you begin:

- Understand custom policy application. See "Understanding Custom Policy Applications" on page 86.
- Understand the ICMP predefined policy application. See "Understanding ICMP Predefined Policy Applications" on page 76.

Overview

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

- There are different message types within ICMP. For example:
  - type 0 = Echo Request message
  - type 3 = Destination Unreachable message
- An ICMP message type can also have a message code. The code provides more specific information about the message, as shown in Table 17 on page 83.

  Table 17: Message Descriptions

Message Type	Message Code
5 = Redirect	0 = Redirect datagram for the network (or subnet)

Table 17: Message Descriptions *(Continued)*

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

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

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

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

Configuration

IN THIS SECTION

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 define a custom ICMP application:

1. Set the application type and code.

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

2. Set the inactivity timeout value.

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

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

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

Verification

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

RELATED DOCUMENTATION

Address Books and Address Sets | 26

Custom Policy Applications

IN THIS SECTION

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

Understanding Custom Policy Applications

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

You can assign each custom application the following attributes:

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

Custom Application Mappings

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

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

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

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

Example: Adding and Modifying Custom Policy Applications

IN THIS SECTION

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

Requirements

Before you begin, create addresses and security zones. See "Example: Creating Security Zones" on page 9.

Overview

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

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

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

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

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

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

To add and modify a custom policy application:

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

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

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

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

3. Modify the custom policy application `cust-telnet` :

- Delete the source and destination ports configured for TCP.
- Configure UDP and specify the source port and destination port.
- Specify the length of time that UDP is inactive.

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

```
destination-port 11000
user@host# set inactivity-timeout 1500
```

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

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

Verification

IN THIS SECTION

Verifying The Modified Custom Policy Application

Purpose

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

Action

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

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

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

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

Meaning

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

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

SEE ALSO

Security Policies Overview | 2
Security Policy Applications Overview | 55
Understanding Custom Policy Applications | 86
Example: Defining a Custom ICMP Application | 83

Example: Configuring Custom Policy Application Term Options

IN THIS SECTION

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

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall
- A PC

Before you begin:

- Configure the required applications. See "Example: Adding and Modifying Custom Policy Applications" on page 87 .

Overview

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

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

Configuration

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.

```
user@host# set applications application app-name term custom-options
user@host# set applications application app-name term custom-options alg dns
user@host#set applications application app-name term custom-options protocol udp
user@host#set applications application app-name term custom-options source-port 24000
user@host#set applications application app-name term custom-options destination-port 23000
user@host#set applications application app-name term  custom-options inactivity-timeout 60
```

Step-by-Step Procedure

To configure custom policy application term options:

1. Configure the term name.

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

2. Configure the ALG type.

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

3. Configure the networking protocol type.

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

4. Configure the source port number.

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

5. Configure the TCP or UDP destination port number.

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

6. Specify the inactivity timeout value.

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

Results

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

```
[edit]
    user@host# show applications
    application app-name {
    term custom-options alg dns protocol udp source-port 24000 inactivity-timeout 60;
}
```

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

Verification

IN THIS SECTION

Verifying the Configuration

Purpose

Verify that the configuration is correct.

Action

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

```
user@host> show applications
    application app-name {
    term custom-options alg dns protocol udp source-port 24000 inactivity-timeout 60;
}
```

RELATED DOCUMENTATION

Security Policy Applications and Application Sets | 55

5

CHAPTER

Security Policies

IN THIS CHAPTER

Configuring Security Policies

IN THIS SECTION

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

Understanding Security Policy Elements

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

Each policy consists of:

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

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

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

Understanding Security Policy Rules

IN THIS SECTION

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

Each policy is associated with the following characteristics:

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

- One or many destination address names or address set names
- One or many application names or application set names

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

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

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

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

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

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

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

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

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

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

Policy look up determines the destination zone, destination address, and egress interface.

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

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

  Any policy configured with the `to-zone` as a global zone must have a single destination address to indicate that either static NAT or incoming NAT has been configured in the policy.
- The policy permit option with NAT is simplified. Each policy will optionally indicate whether it allows NAT translation, does not allow NAT translation, or does not care.

- Address names cannot begin with the following reserved prefixes. These are used only for address NAT configuration:
  - `static_nat_`
  - `incoming_nat_`
  - `junos_`
- Application names cannot begin with the `junos_` reserved prefix.

Understanding Wildcard Addresses

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

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

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

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

NOTE: Content Security for IPv6 sessions is not supported. If your current security policy uses rules with the IP address wildcard any, and Content Security features are enabled, you will encounter configuration commit errors because Content Security features do not yet support IPv6 addresses. To resolve the errors, modify the rule returning the error so that the any-ipv4 wildcard is used; and create separate rules for IPv6 traffic that do not include Content Security features.

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

SEE ALSO

View and Change Security Policy Ordering | 223

Policy Configuration Synchronization Enhancements

IN THIS SECTION

Enhanced policy configuration synchronization mechanism improves how policy configurations are synchronized between the Routing Engine (RE) and the Packet Forwarding Engine (PFE), enhancing system reliability and security. This mechanism ensures policies are automatically and accurately synchronized. In addition, the system effectively prevents any flow-drops during the security policy configuration change process.

File-Serialization

Perform policy changes propagation to the dataplane using file-serialization. By serializing policy configurations into files, the system ensure that they are read and applied by the PFE in a controlled and reliable manner. These serialized files are stored in designated directories and are automatically deleted after successful application, providing a more efficient and bandwidth-friendly method of synchronization. This file-based approach reduces the risk of security policy mismatches and enhances system reliability.

By default, the file-based serialization is enabled. You can disable the file-serialization by using the following statement:

```
[edit]
user@host# set security policies no-file-serialization
```

To re-enable the file-serialization feature, use the following statement:

```
[edit]
user@host# delete security policies no-file-serialization
```

Or use the following statement:

```
[edit]
user@host# set security policies file-serialization
```

Prevent Flow Session Disruption During Policy Configuration Changes

You can avoid flow session disruption during security policy configuration changes commit. Configuration changes, such as policy match condition or action changes, addition or deletion of a policy, policy swap or change in policy order disrupts flow sessions. These changes affect PFE configuration data, potentially impacting ongoing policy searches and possibly leading to incorrect or default policy selection. That is, during the brief transition from old to new policy, sessions might match partially created data structures, causing incorrect policy matches.

To avoid the disruption caused by security policy change, you can use the following statement:

```
[edit]
user@host# set security policies lookup-intact-on-commit
```

When you configure the `lookup-intact-on-commit` option, restart the forwarding plane on the device or in a chassis cluster setup.

Use the following command to check the status and eligibility of the device before enabling the `lookup-intact-on-commit` option.

```
[edit]
user@host> show security policies lookup-intact-on-commit
```

The command output displays if the `lookup-intact-on-commit` option is already configured on the device and displays eligibility of the device in terms of available memory storage for activating `lookup-intact-on-commit` option.

Memory and Error Handling

Implementing these new synchronization mechanisms requires your system to meet specific memory requirements. Specifically, you need at least 5 percent free kernel heap and 1 percent free user heap to enable the lookup-intact-on-commit feature. This ensures that there is sufficient memory available for the file-based synchronization and dual-memory operations. In case of synchronization failures, the system is designed to automatically revert to the traditional method.

You can use the `show security policies lookup-intact-on-commit eligibility`command to check the memory availability of the system per FPC. This output indicates if the particular FPC is eligible for configuring the `set security policies lookup-intact-on-commit` configuration.

Support for Logical System and Tenant System

You can configure `lookup-intact-on-commit` and `file-serialization` at the root logical system (system-level) only. Configuration at the logical-system and tenant-system levels is not supported. However, if you configure these settings at the root level, the configuration will also optimize policies configured at logical-system and tenant-system levels.

Understanding Security Policies for Self Traffic

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

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

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

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

The advantages of using the self-traffic are:

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

> **NOTE**: The default security policy rules do not affect self-traffic.

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

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

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

Security Policies Configuration Overview

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

1. Create zones. See "Example: Creating Security Zones" on page 9.
2. Configure an address book with addresses for the policy. See "Example: Configuring Address Books and Address Sets" on page 36.
3. Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 56.
4. Create the policy. See "Example: Configuring a Security Policy to Permit or Deny All Traffic" on page 107, "Example: Configuring a Security Policy to Permit or Deny Selected Traffic" on page 113, and "Example: Configuring a Security Policy to Permit or Deny Wildcard Address Traffic" on page 120.

5. Create schedulers if you plan to use them for your policies. See "Example: Configuring Schedulers for a Daily Schedule Excluding One Day" on page 227.

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

SEE ALSO

Troubleshoot Security Policies | 427

Best Practices for Defining Policies

A secure network is vital to a business. To secure a network, a network administrator must create a security policy that outlines all of the network resources within that business and the required security level for those resources. The security policy applies the security rules to the transit traffic within a context (from-zone to to-zone) and each policy is uniquely identified by its name. The traffic is classified by matching the source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Platform support depends on the Junos OS release in your installation.

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

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

- Policy context–Used to organize all policies in this context. Policy context includes variables such as source and destination zones.

- Policy entity–Used to hold the policy data. Policy entity calculates memory using parameters such as policy name, IP addresses, address count, applications, firewall authentication, WebAuth, IPsec, count, application services, and Junos Services Framework (JSF).

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

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

Memory is also consumed by the "deferred delete" state. In the deferred delete state, when a device applies a policy change, there is transitory peak usage whereby both the old and new policies are present. So for a brief period, both old and new policies exist on the Packet Forwarding Engine, taking up twice the memory requirements.

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

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

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

> **NOTE**: The memory requirement for each device is different. Some devices support 512,000 sessions by default, and the bootup memory is usually at 72 to 73 percent. Other devices can have up to 1 million sessions and the bootup memory can be up to 83 to 84 percent. In the worst-case scenario, to support about 80,000 policies in the

SPU, the SPU should boot with a flowd kernel memory consumption of up to 82 percent, and with at least 170 megabytes of memory available.

SEE ALSO

Understanding Global Address Books | 29
Global Policy Overview | 184
Checking Memory Usage | 421

Configuring Policies Using the Firewall Wizard

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

To configure policies using the Firewall Policy Wizard:

1. Select `Configure>Tasks>Configure FW Policy` in the J-Web interface.
2. Click the Launch Firewall Policy Wizard button to launch the wizard.
3. Follow the prompts in the wizard.

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

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

IN THIS SECTION

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

Requirements

Before you begin:

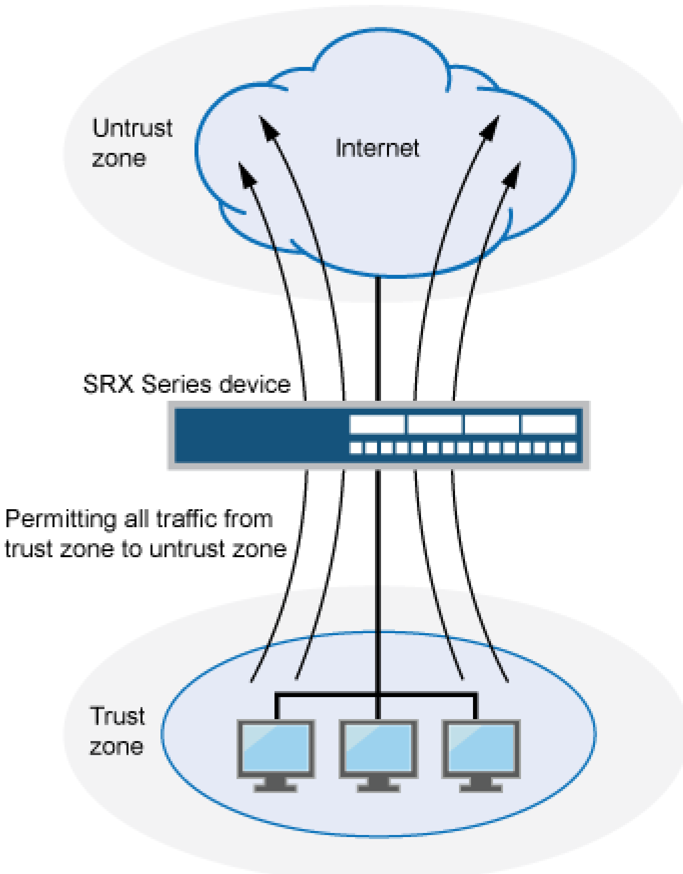
- Create zones. See "Example: Creating Security Zones" on page 9.
- Configure an address book and create addresses for use in the policy. See "Example: Configuring Address Books and Address Sets" on page 36.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 56.

Overview

IN THIS SECTION

In the Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on traffic as it passes through the device. From the perspective of security policies, the traffic enters one security zone and exits another security zone. In this example, you configure the trust and untrust interfaces, ge-0/0/2 and ge-0/0/1. See Figure 4 on page 109.

Figure 4: Permitting All Traffic



This configuration example shows how to:

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

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

Step-by-Step Procedure

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

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

1. Configure the interfaces and security zones.

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

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

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

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

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

Results

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

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

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

```
}
from-zone untrust to-zone trust {
    policy deny-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}
```

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

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

Meaning

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

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

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

IN THIS SECTION

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

Requirements

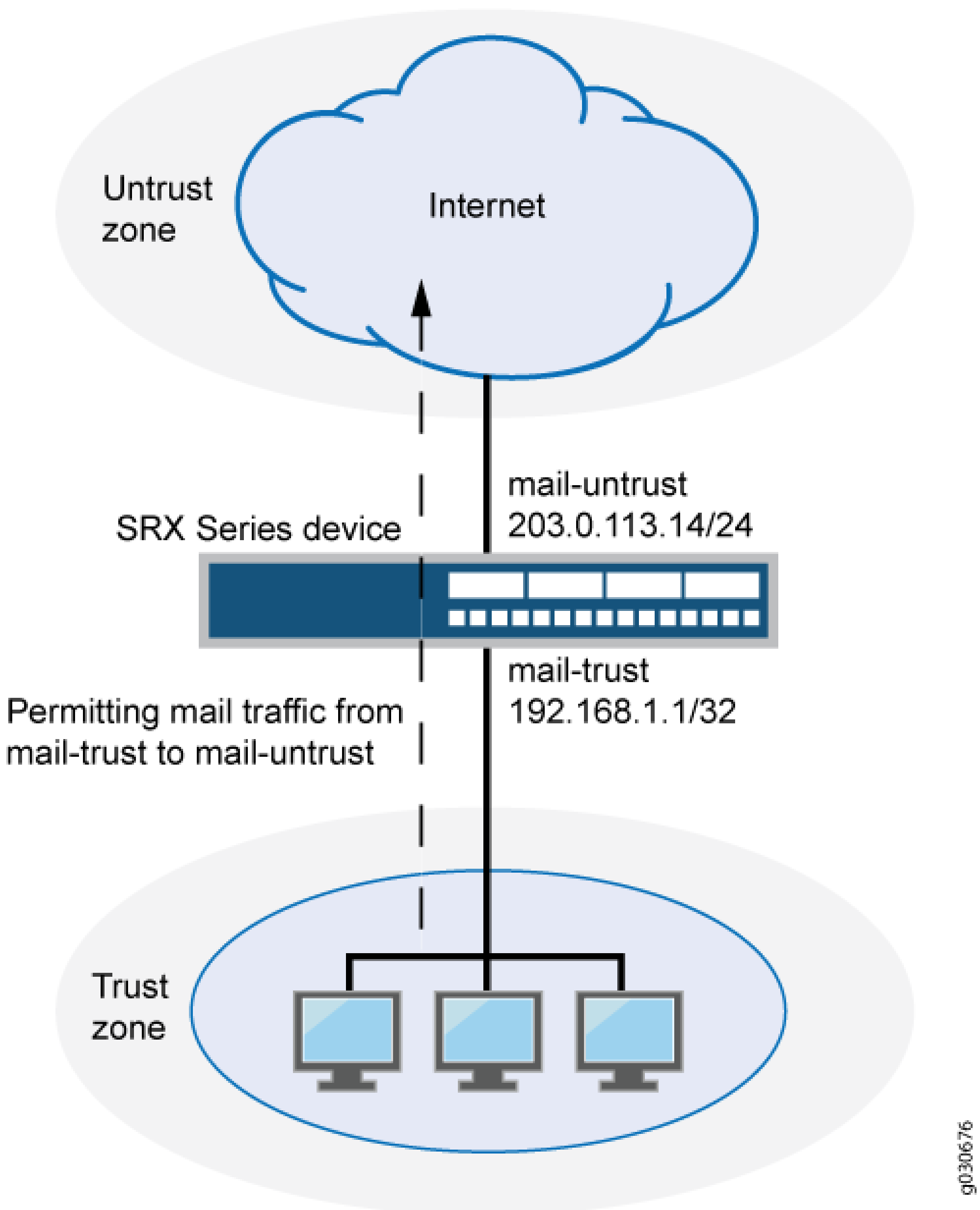
Before you begin:

- Create zones. See "Example: Creating Security Zones" on page 9.
- Configure an address book and create addresses for use in the policy. See "Example: Configuring Address Books and Address Sets" on page 36.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 56.
- Permit traffic to and from trust and untrust zones. See "Example: Configuring a Security Policy to Permit or Deny All Traffic" on page 107.

Overview

In Junos OS, security policies enforce rules for the transit traffic, in terms of what traffic can pass through the device, and the actions that need to take place on the traffic as it passes through the device. From the perspective of security policies, the traffic enters one security zone and exits another security zone. In this example, you configure a specific security policy to allow only e-mail traffic from a host in the trust zone to a server in the untrust zone. No other traffic is allowed. See Figure 5 on page 115.

Figure 5: Permitting Selected 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 security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services
all
set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic system-
services all
set security address-book book1 address mail-untrust 203.0.113.14/24
set security address-book book1 attach zone untrust
set security address-book book2 address mail-trust 192.168.1.1/32
set security address-book book2 attach zone trust
set security policies from-zone trust to-zone untrust policy permit-mail match source-address
mail-trust
set security policies from-zone trust to-zone untrust policy permit-mail match destination-
address mail-untrust
set security policies from-zone trust to-zone untrust policy permit-mail match application junos-
mail
set security policies from-zone trust to-zone untrust policy permit-mail then permit
```

Step-by-Step Procedure

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

To configure a security policy to allow selected traffic:

1. Configure the interfaces and security zones.

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

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

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

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

3. Define the policy to permit mail traffic.

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

Results

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

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

```
    }
}
```

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

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

```
        attach {
            zone trust;
        }
    }
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

Meaning

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

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

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

IN THIS SECTION

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

Requirements

Before you begin:

- Understand wildcard addresses. See "Understanding Security Policy Rules" on page 97.
- Create zones. See "Example: Creating Security Zones" on page 9.
- Configure an address book and create addresses for use in the policy. See "Example: Configuring Address Books and Address Sets" on page 36.
- Create an application (or application set) that indicates that the policy applies to traffic of that type. See "Example: Configuring Security Policy Applications and Application Sets" on page 56.
- Permit traffic to and from trust and untrust zones. See "Example: Configuring a Security Policy to Permit or Deny All Traffic" on page 107.
- Permit e-mail traffic to and from trust and untrust zones. See "Example: Configuring a Security Policy to Permit or Deny Selected Traffic" on page 113

Overview

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

Configuration

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` in configuration mode.

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

Step-by-Step Procedure

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

To configure a security policy to allow selected traffic:

1. Configure the interfaces and security zones.

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

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

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

3. Define the policy to permit wildcard address traffic.

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

Results

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

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

```
            permit;
        }
    }
}
```

```
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        interfaces {
            ge-0/0/2 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
}
    security-zone untrust {
        interfaces {
            ge-0/0/1 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                }
            }
        }
    }
user@host# show security address-book
book1 {
    address wildcard-trust {
        wildcard-address 192.168.0.11/255.255.0.255;
    }
    attach {
        zone trust;
```

```
    }
}
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

Meaning

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

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

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

IN THIS SECTION

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

Requirements

This example uses the following hardware and software components:

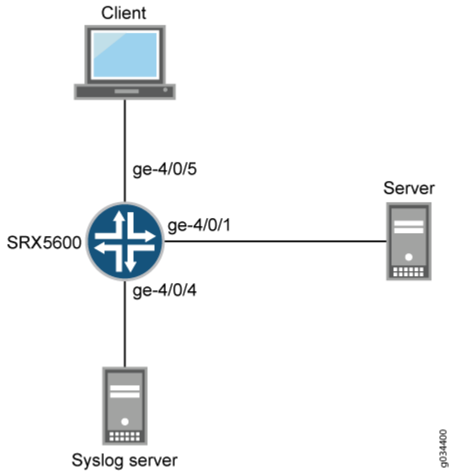
- A client connected to an SRX5600 device at the interface ge-4/0/5
- A server connected to the SRX5600 device at the interface ge-4/0/1

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

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

Overview

In this example, you configure a security policy on the SRX5600 device to send traffic logs, generated by the device during data transmission, to a Linux-based server. Traffic logs record details of every session. The logs are generated during session establishment and termination between the source and the destination device that are connected to the SRX5600 device.



Configuration

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` in configuration mode.

```
set security log source-address 127.0.0.1
set security log stream trafficlogs severity debug
set security log stream trafficlogs host 203.0.113.2
set security zones security-zone client host-inbound-traffic system-services all
set security zones security-zone client host-inbound-traffic protocols all
set security zones security-zone client interfaces ge-4/0/5.0
set security zones security-zone server host-inbound-traffic system-services all
set security zones security-zone server interfaces ge-4/0/4.0
set security zones security-zone server interfaces ge-4/0/1.0
set security policies from-zone client to-zone server policy policy-1 match source-address any
set security policies from-zone client to-zone server policy policy-1 match destination-address
any
```

```
set security policies from-zone client to-zone server policy policy-1 match application any
set security policies from-zone client to-zone server policy policy-1 then permit
set security policies from-zone client to-zone server policy policy-1 then log session-init
set security policies from-zone client to-zone server policy policy-1 then log session-close
```

Step-by-Step Procedure

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

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

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

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

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

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

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

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

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

```
[edit security policies from-zone client to-zone server]
user@host# set policy policy-1 match source-address any
user@host# set policy policy-1 match destination-address any
user@host# set policy policy-1 match application any
user@host# set policy policy-1 match then permit
```

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

```
[edit security policies from-zone client to-zone server]
user@host# set policy policy-1 then log session-init
user@host# set policy policy-1 then log session-close
```

Results

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

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

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying Zones

Purpose

Verify that the security zone is enabled or not.

Action

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

Verifying Policies

Purpose

Verify that the policy is working.

Action

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

TAP Mode for Security Zones and Policies

IN THIS SECTION

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

Understanding TAP Mode Support for Security Zones and Policies

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

When you configure a device to operate in TAP mode, the device generates security log information to display the information on threats detected, application usage, and user details. When the device is configured to operate in TAP mode, the device receives packets only from the configured TAP interface. Except the configured TAP interface, other interface are configured to normal interface that is used as management interface or connected to the outside server. The device generates security report or log according to the incoming traffic.

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

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

Example: Configuring Security Zones and Policies in TAP mode

IN THIS SECTION

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

Requirements

This example uses the following hardware and software components:

- An SRX Firewall
- Junos OS Release 19.1R1

Overview

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

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

```
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-init
set security policies from-zone tap-zone to-zone tap-zone policy tap-policy then log session-
close
```

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 zones in TAP mode:

1. Configure security zone tap-zone interface.

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

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

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

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

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

Results

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

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

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

Verification

IN THIS SECTION

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

Verifying Policy Configuration in TAP Mode

Purpose

Verify information about security policies.

Action

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

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

```
  any-ipv6(global): ::/0
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
```

Meaning

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

Dynamic Address Groups in Security Policies

IN THIS SECTION

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

The following types of IP addresses are supported:

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

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

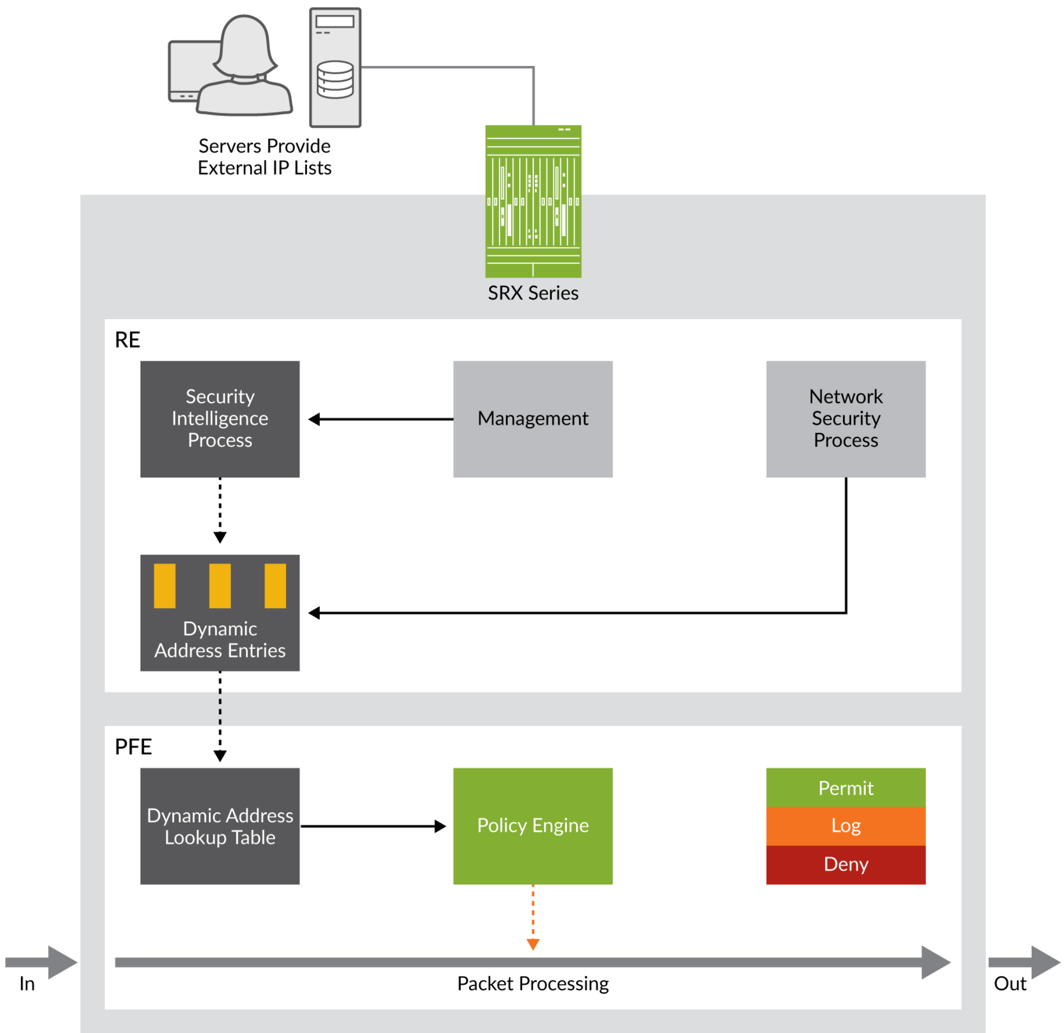
NOTE: A dynamic address entry is a group of IP addresses, not a single IP prefix. A dynamic address entry is different from the security address concepts of address books and address entry addresses.

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

- The network administrator has more control over the traffic to and from groups of IP addresses.
- The external server provides updated IP address feeds to the SRX Firewall.
- The administrator's efforts are dramatically reduced. For example, in a legacy security policy configuration, adding 1000 address entries for a policy to reference would require some 2000 lines of configuration. By defining a dynamic address entry and referencing it in a security policy, up to millions of entries could flow into the SRX Firewall without much additional configuration effort.
- No commit process is required to add new addresses. Adding thousands of addresses to a configuration through a legacy method takes a long time to commit. Alternatively, IP addresses in a dynamic address entry come from an external feed, so no commit process is required when the addresses in an entry change.

Figure 6 on page 137 illustrates a functional overview of how the dynamic address entry in a security policy works.

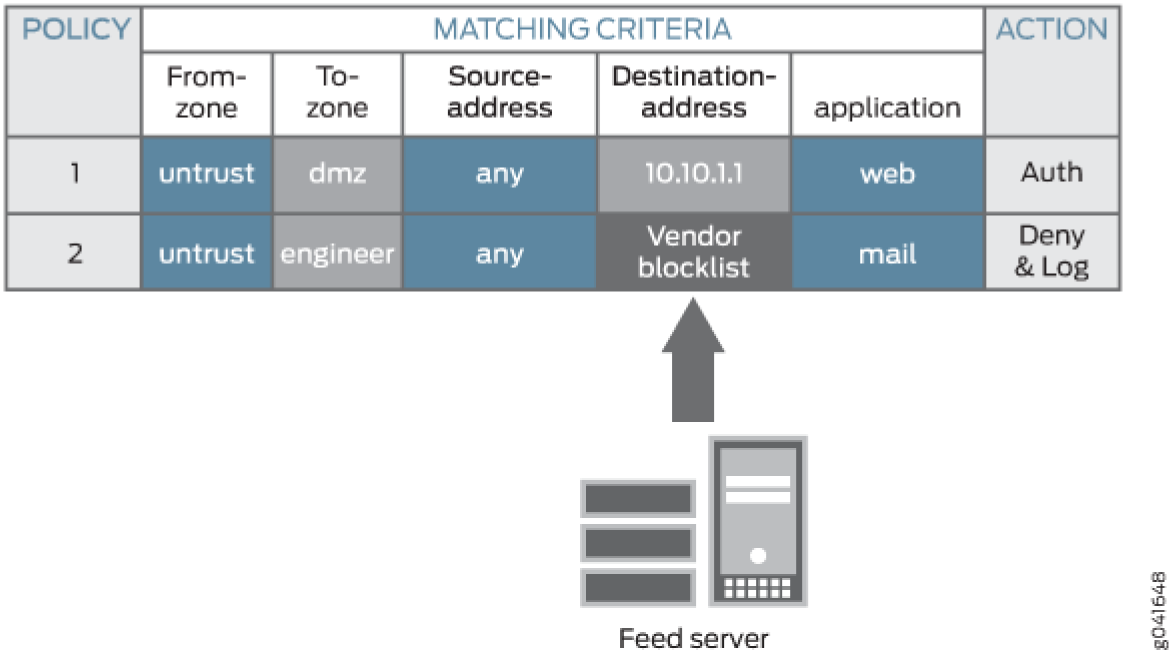
Figure 6: Functional Components of the Dynamic Address Entry in a Security Policy



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

Figure 7 on page 138 illustrates a policy that uses a dynamic address entry in the Destination-address field.

Figure 7: A Dynamic Address Entry in a Security Policy



In Figure 7 on page 138, Policy 1 uses the destination address 10.10.1.1, which is a legacy security address entry. Policy 2 uses the destination address Vendor blocklist, which is a dynamic address entry named by the network administrator. Its content is the list of IP addresses retrieved from an external feed file. Packets that match all five criteria (the From-zone named untrust, the To-zone named engineer, any source address, a destination IP address that belongs to the Vendor blocklist dynamic address entry, and the mail application) are handled according to the policy actions, which are to deny and log the packet.

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

Dynamic address groups support the following data feeds:

- Custom lists (allowlists and blocklists)
- GeoIP

Feed Servers

- Feed servers contain dynamic address entries in a feed file. You can create custom feeds which can be local or remote. For custom feeds creation, see, Creating Custom Feeds
- Configure the SRX Firewall for using the feeds. See, *feed-server* to configure SRX Firewall.

Bundle Feeds

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

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

The following bundle feed modes are supported:

Archive Mode

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

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

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

  1. Place all feed files for the SRX Firewall under the folder *feeds-4-srx*
  2. Generate all feed files fd1 fd2 fd3 ..fdN in the folder *feeds-4-srx*
  3. Add or remove the IP ranges from the feeds
  4. Access the files by running the following command: `cd feeds-4-srx;tar -zcvf ../feeds-4-srx.tgz *;cd-`
- Post Step 4, the file *feeds-4-srx.tgz* is ready for download on the SRX Firewall containing the same folder which contains the *feeds-4-srx.tgz* file. After the download, the extracted files are placed in the same folder as *feeds-4-srx.tgz*. The following example shows a samle configuration on an SRX Firewall:

```
[edit]
```

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

set security dynamic-address feed-server server-4-srx feed-name feed1 path fd1

set security dynamic-address feed-server server-4-srx feed-name feed2 path fd2

set security dynamic-address feed-server server-4-srx feed-name feed3 path fdN
```

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

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

```
[edit]

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

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

```
[edit]

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

- You can authenticate dynamic address feed servers before downloading feeds into the vSRX 3.0, using the `username` and `password` options. These new authentication options allow you to securely obtain feeds from local or remote web servers, facilitating automatic scaling of business operations and Layer 7 services.

  This configuration ensures that the firewall authenticates the specified feed server before downloading any dynamic address feeds, thereby securing the feed data and maintaining network integrity.

  This command allows you to specify the server name, along with the necessary credentials, ensuring that only authenticated servers are accepted.

  ```
  set security dynamic-address feed-server <feed-server> user-name <user-name>
  ```

  ```
  set security dynamic-address feed-server <feed-server> passowrd <password>
  ```

  NOTE: User name can be minimum of 3 and upto 32 characters long and password can be minimum of 6 and upto 32 characters long that should include only lowercase letters (a-z), uppercase letters (A-Z), and digits (0-9).

Flat File Mode

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

The lines below this tag are regarded as IP ranges belonging to the feed. An example of the file format looks is given below:

```
root>cat feeds-4-srx.bundle

FEED:fd1

12.1.1.1-12.1.1.2

11.1.1.1-11.1.1.2
```

```
FEED:fd2
```

```
14.1.1.1-14.1.1.2
```

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

```
[edit]
set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-srx.bundle
set security dynamic-address feed-server server-4-srx feed-name fd1 path fd1
set security dynamic-address feed-server server-4-srx feed-name fd2 path fd2
```

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

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

```
[edit]
set security dynamic-address feed-server server-4-srx url 10.170.40.50/feeds-4-
srx.bundle.gz
set security dynamic-address feed-server server-4-srx feed-name fd1 path fd1
```

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

Platform-Specific Security Policy Behavior

IN THIS SECTION

Use Feature Explorer to confirm platform and release support for specific features.

Use the following tables to review platform-specific behavior for your platform:

Platform-Specific Security Policies Support

Platform	Difference
SRX Series	The number of security policies and the maximum number of policies per context for SRX5400 devices are 100,000.

Platform-Specific Security Policy Configuration Behavior

Platform	Difference
SRX Series	• On SRX5400 devices that support security policy configuration rules, the policies are looked up during flow processing after firewall filters and screens have been processed and when route look up is been completed by the Services Processing Unit (SPU).
vSRX 3.0 Virtual Firewall	• vSRX 3.0 Virtual Firewall 3.0—the current version of Juniper Networks® vSRX Virtual Firewall—supports Geneve flow infrastructure for Geneve tunnel packet processing. See Geneve Flow Infrastructure on vSRX Virtual Firewall 3.0 and AWS Gateway Load Balancing with Geneve.

Platform-Specific Policy Configuration Synchronization Behavior

Platform	Difference
SRX Series and vSRX 3.0 Virtual Firewall	• SRX1500, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, and vSRX3.0 that support policy configuration synchronization, support the policy lookup intact on commit (`lookup-intact-on-commit`) option. • SRX Firewalls and vSRX3.0 that support policy configuration synchronization, also support file-serialization.

Platform-Specific IDP Support Behavior

Platform	Difference
SRX Series	• SRX5400, SRX5600, and SRX5800 devices that support Intrusion and Prevention (IDP) also handle IDP for IPv6 sessions.

Platform-Specific Firewall Policy Wizard Support Behavior

Platform	Difference
SRX Series	• SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550M devices that support firewall policy wizard, also support J-Web.

Additional Platform Information

Use Feature Explorer to confirm platform and release support for specific features. Additional platforms may be supported.

SRX Firewalls and vSRX 3.0 Virtual Firewall that support file feed server, support:	SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M	SRX1500	SRX4100, SRX4200, SRX4600, SRX5400 devices, and vSRX 3.0	SRX4700
Maximum number of feed servers	10	40	100	5000
Maximum number of feeds	500	200	5000	5000

(Continued)

SRX Firewalls and vSRX 3.0 Virtual Firewall that support file feed server, support:	SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M	SRX1500	SRX4100, SRX4200, SRX4600, SRX5400 devices, and vSRX 3.0	SRX4700
Maximum Number of dynamic addresses entries	500	200	5000	5000

SRX Firewalls that support Policy Object, support:	SRX300 and SRX320	SRX340	SRX345 and SRX380	SRX550 M	SRX1500, SRX1600, and SRX4100	SRX4200 and SRX4300	SRX4600	SRX4700, SRX5400, SRX5600, and SRX5800
Address Objects	2048	2048	2048	2048	4096	4096	4096	16384
Applicati on Objects	128	128	128	128	3072	3072	3072	3072
Security Policies	1024	2048	4096	10240	16000	60000	80000	100000
Policy Contexts (zone pairs)	256	512	1024	2048	4096	4096	8192	8192
Policies Per Context	1024	2048	4096	10240	16000	60000	80000	100000

(Continued)

SRX Firewalls that support Policy Object, support:	SRX300 and SRX320	SRX340	SRX345 and SRX380	SRX550 M	SRX1500, SRX1600, and SRX4100	SRX4200 and SRX4300	SRX4600	SRX4700, SRX5400, SRX5600, and SRX5800
Policies with Counting Enabled	256	256	256	10240	1024	1024	1024	1024

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

RELATED DOCUMENTATION

Security Zones | 7

Global Security Policies | 183

User Role Firewall Security Policies | 195

Unified Security Policies

IN THIS SECTION

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

Unified Policies Overview

IN THIS SECTION

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

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

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

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

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

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

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

Benefits

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

Before Using Unified Policies on SRX Firewalls

With introduction of unified policies in Junos OS Release 18.2, some of the commands are deprecated—rather than immediately removed—to provide backward compatibility. This enables you to bring your old configuration into compliance with the new configuration.

When you upgrade to Junos OS Releases 19.4R3 or 20.2R3, the security device displays the following warning when you try to commit the configuration that includes the deprecated commands:

```
#show security
appliction-firewall {## warning: 'application-firewall' is deprecated
```

We recommend that you migrate to unified policies to bring your configuration up to date with supported features.

The following sections provide details about unsupported configurations in the older release and how you can enable them with the new release.

Application Security

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
Configure individual application firewall rules to allow or reject traffic based on applications. • Configure rules and rule sets at the `set security application-firewall` hierarchy level. • Apply application firewall functionality `set security policies from-zone <zone> to-zone <zone> policy <policy> then permit application-services application-firewall rule-set`.	Create security policies with dynamic applications as match criteria to get the same functionality as application firewall. `set security policies from-zone <zone> to-zone <zone> policy <policy> match dynamic-application <application-name>`

Example: The following samples show the difference in application firewall configuration with 15.1X49 and configuration in 19.4R3-S1 in unified policies. We're using an example of setting up application firewall rules to block Facebook applications.

Before Upgrade

```
set security policies from-zone untrust to-zone trust policy policy1 match source-address any
set security policies from-zone untrust to-zone trust policy policy1 match destination-address
any
set security policies from-zone untrust to-zone trust policy policy1 match application junos-http
set security policies from-zone untrust to-zone trust policy policy1 then permit application-
services application-firewall rule-set rs1
set security application-firewall rule-sets rs1 rule r1 match dynamic-application
[junos:FACEBOOK-ACCESS]
set security application-firewall rule-sets rs1 rule r1 then deny
set security application-firewall rule-sets rs1 default-rule permit
```

After Upgrade

```
set security policies from-zone trust to-zone untrust policy policy-1 match source-address any
set security policies from-zone trust to-zone untrust policy policy-1 match destination-address
any
set security policies from-zone trust to-zone untrust policy policy-1 match application any
set security policies from-zone trust to-zone untrust policy policy-1 match dynamic-application
junos:FACEBOOK-ACCESS
```

```
set security policies from-zone trust to-zone untrust policy policy-1 then reject profile
profile1
```

IDP Policies

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
Assign an IDP policy as the active IDP policy and use it as match criteria in a security policy to perform intrusion detection and prevention.	Configure multiple IDP policies and apply them to the security policy. You can even define one of the IDP policies as the default policy.

• Specify an active IDP policy:
`set security idp active-policy <IDP policy name>`
• Apply IDP policy in the security policy:
`set security policies from-zone <zone> to-zone <zone> policy <policy> then permit application-services idp`
	Specify multiple IDP policies per firewall rule:
	`set security policies from-zone <zone> to-zone <zone> policy <policy-1> then permit application-services <IDP-policy-name-1>`
	`set security policies from-zone <zone> to-zone <zone> policy <policy-2> then permit application-services <IDP-policy-name-2>`
	`set security idp default-policy <IDP-policy name>`

Example: The following samples show the difference in IDP configuration with 15.1X49 and configuration in 19.4R3 in unified policies. Note that, in unified policies, you have the flexibility to configure multiple IDP policies.

Before Upgrade

```
set security idp active-policy recommended
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match source-address
any
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match destination-
address any
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 match application
junos:GMAIL
set security policies from-zone Zone1 to-zone Zone2 policy idp-app-policy-1 then permit
application-services idp
```

After Upgrade

```
set security idp idp-policy recommended
set security idp idp-policy idpengine
set security idp default-policy recommended
set from-zone trust to-zone untrust policy P2 match source-address any
set from-zone trust to-zone untrust policy P2 match destination-address any
set from-zone trust to-zone untrust policy P2 match application junos-defaults
set from-zone trust to-zone untrust policy P2 match dynamic-application junos:GMAIL
set from-zone trust to-zone untrust policy P1 then permit application-services idp-policy
recommended
set from-zone trust to-zone untrust policy P2 then permit application-services idp-policy
idpengine
```

Content Security

Junos OS Release 15.1X49	Unified Policies (Post Junos OS Release 18.2)
Configure Content Security feature parameters under each feature profile. • `set security utm feature-profile anti-virus` • `set security utm feature-profile anti-spam` • `set security utm feature-profile web-filtering` • `set security utm feature-profile content-filtering`	Configure Content Security features under the default configuration. Content Security default configuration applies parameters that you might have missed configuring for a specific Content Security feature. • `set security utm default-configuration anti-virus` • `set security utm default-configuration anti-spam` • `set security utm default-configuration web-filtering` • `set security utm default-configuration content-filtering`

Example: The following samples show the difference in Content Security configuration with 15.1X49 and configuration in 19.4R3-S1 in unified policies. We're using an example of configuration of Sophos antivirus on your security device.

Before Upgrade

```
edit security utm feature-profile anti-virus mime-whitelist
```

```
edit security utm feature-profile anti-virus url-whitelist
edit security utm feature-profile anti-virus sophos-engine
```

After Upgrade

```
edit security utm default-configuration anti-virus mime-whitelist
edit security utm default-configuration anti-virus url-whitelist
edit security utm default-configuration anti-virus sophos-engine
```

Unified Policies Configuration Overview

IN THIS SECTION

The following sections provide more information on unified policies:

Dynamic Application Configuration Options

Table 18 on page 155 provides options for configuring a unified policy with dynamic applications.

Table 18: Dynamic Application Configuration Options

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

Starting in Junos OS Releases 19.4R1 and 20.1R1, security policy does not support using following applications as dynamic-applications match criteria:

- junos:HTTPS
- junos:POP3S
- junos:IMAPS
- junos:SMTPS

Software upgrade to the Junos OS Releases 19.4R1 and 20.1R1 and later releases fails during the validation if any of the security policies are configured with junos:HTTPS, junos:POP3S, junos:IMAPS, junos:SMTPS as dynamic-applications as match criteria.

We recommend you to use the`request system software validate package-name` option before upgrading to the above mentioned releases.

We recommend you to remove any configuration that includes the dynamic-application junos:HTTPS, junos:IMAPS, junos:SMTPS or junos:POP3S as match criteria in security policies.

Default Ports and Protocols as Application Matching Criteria

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

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

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

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

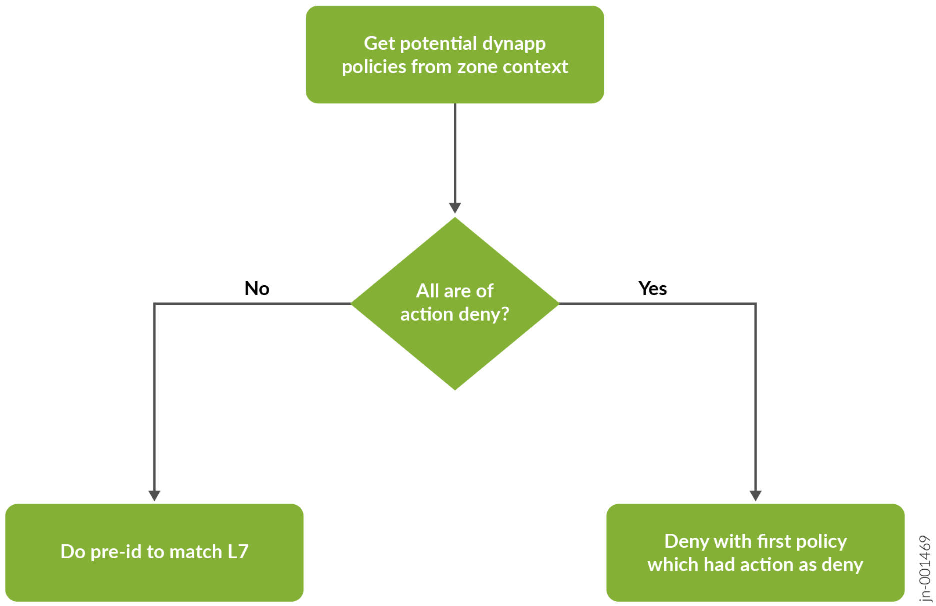
The `junos-defaults` option must be configured along with a dynamic application. If you configure the `junos-defaults` option without specifying any dynamic application, then an error message displays and the configuration commit fails. Use the `show security policies detail` command to validate the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

Pre-ID Default Policy

A unified policy leverages the information from AppID to match the application and take action as specified in the policy. Before identifying the final application, the policy cannot be matched precisely.

Starting in Junos OS Release 23.4R1, the flow process is optimized to deny the traffic (without AppID) when all the potential policies (including the default policy) would deny the traffic.

Figure 8: Security Policy Selection Optimization



The flow does not proceed to the Pre-ID default policy pre-id-default-policy) but is instead denied by the default policy or by the topmost rule in the unified policy. The sessions matching Pre-Id default Policy are denied if there is no potential permit policy before performing application identification (AppID).

When the device receives the first packet of a traffic flow, it performs the basic 5-tuple matching and checks the defined potential policies to determine how to treat the packet. If all potential policies have the action as "deny", and the default policy action is also set to "deny", then the device denies the traffic and does not perform application identification (AppID).

If any policy has action as other than "deny", then the device performs DPI to identify the application.

The device checks for potential policies on both zone context and global context.

Default Policy Actions Prior to Dynamic Application Identification

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

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

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

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

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

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

Global Policy Utilization with Unified Policies

Zone-based security policies are prioritized over global policies when a policy lookup is implemented.

If the session matches any unified policy, either at a zone-level or at a global-level, then the policy is added to potential policy match list. If the session does not match a policy at zone-level then the next policy match occurs at the global-level. Global-level policies have the same match criteria as any other security policy (example: source address, destination address, application, dynamic-application and so on).

Unified Policy Actions

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

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

Redirect Profile for Reject Action

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

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

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

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

Limitations to Configuring a Redirect Profile in Unified Policies

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

- Support for the redirect action with block messages with a redirect URL are not available for non-HTTP or non-HTTPS applications.
- A unified policy does not check the validity and accessibility of a user-configured redirect URL.
- For clear text processing, out-of-order HTTP packets, or segmented HTTP requests, the available policy actions are reject or deny. A redirect profile is not available.
- The redirect profile can be applied in unified policies only. The reject action for traditional security policies do not support a redirect action with block message profiles or a redirect URL.

SSL Proxy Profile for Reject Action

Starting in Junos OS Release 18.2R1, you can configure a redirect profile within a unified policy. When a policy blocks HTTP or HTTPS traffic with a deny or reject action, you can apply an SSL proxy profile to the traffic. SSL proxy decrypts the traffic and application identification functionality identifies the application. Next, you can take action to redirect or drop the traffic as per the configuration.

Consider the following example:

In this example, you are rejecting some of the Facebook applications such as chat, Farmville, and so on in the policy ’policy-1’. As Facebook is an encrypted application, you need SSL proxy to decrypt the traffic first.

```
policy policy-1 {
    match {
        source-address any;
        destination-address any;
        application any;
        dynamic-application [ junos:FACEBOOK-CHAT junos:FACEBOOK-FARMVILLE junos:FACEBOOK-MOBILE-
CHAT junos:FACEBOOK-SUPERPOKE junos:FACEBOOK-WINDOWSLIVEMESSENGER junos:FACEBOOK-VIDEO ];
    }
    then {
        reject {
            ssl-proxy {
                profile-name test;
            }
        }
        log {
            session-init;
            session-close;
        }
    }
}
```

In this example, the policy rejects the encrypted Facebook traffic and applies the configured SSL proxy profile. The SSL proxy decrypts the traffic, and JDPI identifies the application.

Now the policy takes following actions based on your configuration:

- Redirects the client access to other URL, and closes the original session.
- Notifies the client with pre-defined text messages, and closes the session
- Closes the session only. In the example, the policy closes the session.

Match Criteria and Rules for Unified Policies

Unified Policy Implicit and Explicit Match

Starting in Junos OS Release 18.2R1, the command `unified-policy-explicit-match` is introduced at the `[edit security policies]` hierarchy level. This command defines the explicit and implicit policy match behavior and is disabled by default.

- *Explicit match*—If a dependent application does not have any matching policy, then the traffic is dropped if explicit match is enabled. Only those security policies that are explicitly configured for the application are applied.
- *Implicit Match*—If the dependent application does not have any matching policy, then the security policy that is configured for the base application is applied.

By default, the unified policies enforce implicit rules on dependent applications.

In the example shown in Table 19 on page 161, the unified policy P3 is configured for FACEBOOK-ACCESS traffic. HTTP is a dependent application of FACEBOOK-ACCESS and does not have any security policy explicitly configured for it.

Table 19: Example of an Explicit and Implicit Policy Match for a Dependent Application

Dynamic Application	Policy Configured
HTTP	None
FACEBOOK-ACCESS	P3

The results for implicit and explicit match behavior is shown in Table 20 on page 161.

Table 20: Example of a Policy Match (Implicit and Explicit Match Criteria)

<table>
<tr><th>Application Identified</th><th>Policy Matched</th><th>Explicit or Implicit Rule Type</th><th>Result</th></tr>
<tr><td>None</td><td rowspan="3">P3</td><td rowspan="3">Implicit (Explicit is not Enabled)</td><td rowspan="3">The identified application is HTTP. There is no matching security policy configured for HTTP. The explicit match is not enabled (implicit match), so traffic is further processed until FACEBOOK-ACCESS is identified. The security policy that is configured for FACEBOOK-ACCESS (policy P3) is applied.</td></tr>
<tr><td>HTTP</td></tr>
<tr><td>FACEBOOK-ACCESS</td></tr>
<tr><td>HTTP</td><td>None</td><td>Explicit</td><td>The identified application is HTTP. There is no matching policy available for HTTP. The explicit match is enabled, so no security policy is applied in this case.</td></tr>
</table>

Profile Overlap for Layer 7 Services

While using unified policies, if AppID results have not yet identified the final application, a policy search might return a list of policies instead of a fixed policy. These policies are referred to as potential match policies. Before the final application is identified, a conflict might occur due to multiple policy matches.

In this case, an appropriate profile or default profile is applied for services such as AppQoS, SSL proxy, Content Security, and IDP.

Policy Rematch

When the `policy rematch` option is enabled, the unified policy allows the device to reevaluate an active session when its associated security policy is modified.

The session remains open if it continues to match the policy that allowed the session initially. The session closes if its associated policy is renamed, deactivated, or deleted. Use the `extensive` option to reevaluate an active session when its associated security policy is renamed, deactivated, or deleted.

If policy rematch is configured in a unified policy before a final match, then rematch behavior might lead to a session closure. After the final match, a policy rematch triggers another policy lookup based on the 6-tuple match criteria and the final identified application.

Configure `policy-rematch` and the `policy-rematch` *`extensive`* options at the `[edit security policies]` hierarchy level.

Limitations to Configuring Unified Policies

There are limitations to configuring unified policies. They include:

- An existing session might close in the following cases:
  - When there is a change in the final match for the policy.
  - When a new policy is inserted within the existing policies, and if this new policy is configured with new services.
  - When a final match policy enables new services after the session is created and before the final match.
- Policy-based VPN is not supported for unified policies and can be applied only to the traditional policy.
- ALG traffic processing on the Unified policies does not engage ALG functions.
- ALGs are applied when matching against traditional security policies.
  - Policies using a match condition of `dynamic-application as none` are treated as traditional policies .

- FTP is an exception to ALG support on Unified policies allowing FTP file scanning for Content Security Antivirus.
  - Requires use of `dynamic-application any` or `dynamic-application junos:FTP`.
  - See Enabling FTP Antivirus Scanning (CLI Procedure)
- A security policy that is configured with GPRS might not work if the policy is part of a potential match list.
- A group VPN and user firewall authentication can be applied to a traditional security policy.
- Final policy match information might not be available within session-init logs for policies leveraging dynamic applications.

SEE ALSO

pre-id-default-policy
Unified Policies Support for Flow
profile(dynamic-application)
unified-policy-explicit-match
Understanding Unified Policies [Unified Threat Management (UTM)]
Overview of IDP Policy support for Unified Policies
policy-rematch

Example: Configure a Unified Policy Using a Redirect Message Profile

IN THIS SECTION

This example describes how to configure a unified policy with a redirect message profile. In this example, you configure a redirect profile with a redirect URL. You use the redirect profile as a block message in the policy for traffic in the dynamic applications GMAIL and FACEBOOK-CHAT. Simultaneously, you configure the application `junos-defaults` so that the default port and protocol from the dynamic applications are inherited as the current policy's destination port and protocol match criteria.

Requirements

This example uses the following hardware and software components:

- SRX Firewall running Junos OS Release 18.2R1. This configuration example is tested with Junos OS release 18.2R1.

Before you begin, configure security zones. See "Example: Creating Security Zones" on page 9.

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

Overview

In this example, you define the redirect profile as a response when a policy blocks HTTP or HTTPS traffic with a deny or reject action. Through a redirect profile, you provide an explanation for the action or you redirect the client request to an informative webpage when the reject or deny action is applied in a security policy.

To accomplish these objectives, you perform the following tasks:

- Configure the redirect profile with a redirect URL and use it in the policy as a block message.
- Configure the security policy match criteria `source-address` and `destination-address` with the value `any`.
- Configure the application with `junos-defaults`, so that the default port and protocol from `dynamic-application` is inherited as the current policy's destination port and protocol match criteria.
- Configure `dynamic-application` with `[junos:GMAIL, junos:FACEBOOK-CHAT]` so that the policy can apply the block message profile on the applications.

Configuration

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 security zones security-zone trust
set security zones security-zone untrust
set security dynamic-application profile profile1 redirect-message type redirect-url content
http://abc.company.com/information/block-message
set security policies from-zone trust to-zone untrust policy p2 match source-address any
set security policies from-zone trust to-zone untrust policy p2 match destination-address any
set security policies from-zone trust to-zone untrust policy p2 match application junos-defaults
set security policies from-zone trust to-zone untrust policy p2 match dynamic-application
[junos:GMAIL, junos:FACEBOOK-CHAT]
set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Procedure

Step-by-Step Procedure

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

To configure a unified policy with a redirect message profile:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a profile for the redirect message.

```
[edit security]
user@host# set dynamic-application profile profile1 redirect-message type redirect-url
content http://abc.company.com/information/block-message
```

3. Create a security policy with a dynamic application as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p2 match source-address any
user@host# set from-zone trust to-zone untrust policy p2 match destination-address any
user@host# set from-zone trust to-zone untrust policy p2 match application junos-defaults
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:GMAIL
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application
junos:FACEBOOK-CHAT
```

4. Define the policy action.

```
[edit security policies]
user@host# set security policies from-zone trust to-zone untrust policy p2 then reject
profile profile1
```

Results

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

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


from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;
            application junos-defaults;
            dynamic-application [ junos:GMAIL, junos:FACEBOOK-CHAT ];
        }
        then {
            reject {
                profile profile1;
            }
        }
```

```
    }
}
```

```
[edit]
user@host# show security dynamic-application


    profile profile1 {
        redirect-message {
            type {
                redirect-url {
                    content http://abc.company.com/information/block-message;
                }
            }
        }
    }
```

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

Verification

IN THIS SECTION

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

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

```
user@host> show security policies


Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
 Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
    dynapp-redir-profile: profile1
```

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

```
user@host> show security policies detail


Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
```

```
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
  Dynamic Application:
    junos:GMAIL: 51
  dynapp-redir-profile: profile1
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses
- Configured applications
- Configured dynamic applications
- Policy reject action

SEE ALSO

dynamic-application (Security Policies)

profile(dynamic-application)

Configure a URL Category with Unified Policies

IN THIS SECTION

Understanding URL Category with Unified Policies

IN THIS SECTION

Starting from Junos OS Release 18.4R1, the unified policies feature is enhanced to include URL categories as match criteria for web filtering category. URL categories can be configured to unified policies with or without dynamic-application been applied. .

When the URL category is configured as `url-category` *any* to a policy, the policy matches all categories of traffic configured to the unified policies.

When the URL category is configured as `url-category` *none* to a policy, the URL category is not used in the policy look-up. The unified policy configured with `url-category` *none* is considered as the highest priority to policy match for a traffic. When the URL category to a policy is not configured, or when you upgrade a device from previous release to latest release, the URL category of all the policies are considered as `url-category` *none*.

Limitations of URL Category with Unified Policies

Using URL categories in an unified policy has the following limitation:

- Only the ports that are generally used such as HTTP and HTTPs traffics are supported by `url-category`. Hence, the policy lookup supports HTTP and HTTPs traffics.

Example: Configuring a Unified Policy Using URL Category

IN THIS SECTION

This example describes how to configure a unified policy with a URL category.

Requirements

This example uses the following hardware and software components:

- SRX Firewall running Junos OS Release 18.4R1. This configuration example is tested with Junos OS release 18.4R1.

Before you begin, configure security zones. See "Example: Creating Security Zones" on page 9.

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

Overview

In this example, URL category is added to security policy as match criteria for web filtering category.

To accomplish these objectives, you perform the following tasks:

- Configure the security policy match criteria `source-address` and `destination-address` with the value `any`.
- Configure the application with `junos-defaults`, so that the default port and protocol from `dynamic-application` is inherited as the current policy's destination port and protocol match criteria.
- Configure `dynamic-application` with `[junos:GMAIL, junos:FACEBOOK-CHAT]` so that the policy can apply the block message profile on the applications.
- Configure `url-category` with `Enhanced_News_and_Media` as match criteria for web filtering category.

Configuration

IN THIS SECTION

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

CLI Quick Configuration

```
set security zones security-zone trust
set security zones security-zone untrust
set security policies from-zone trust to-zone untrust policy p2 match source-address any
set security policies from-zone trust to-zone untrust policy p2 match destination-address any
set security policies from-zone trust to-zone untrust policy p2 match application junos-defaults
set security policies from-zone trust to-zone untrust policy p2 match dynamic-application
[junos:GMAIL, junos:FACEBOOK-CHAT]
set security policies from-zone trust to-zone untrust policy p2 match url-category
Enhanced_News_and_Media
set security policies from-zone trust to-zone untrust policy p2 then reject profile profile1
```

Step-by-Step Procedure

Step-by-Step Procedure

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

To configure a unified policy with a redirect message profile:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a security policy with a URL category as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p2 match source-address any
user@host# set from-zone trust to-zone untrust policy p2 match destination-address any
user@host# set from-zone trust to-zone untrust policy p2 match application junos-defaults
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application junos:GMAIL
user@host# set security policies from-zone trust to-zone untrust policy p2 match url-category
Enhanced_News_and_Media
user@host# set from-zone trust to-zone untrust policy p2 match dynamic-application
junos:FACEBOOK-CHAT
```

3. Define the policy action.

```
[edit security policies]
user@host# set security policies from-zone trust to-zone untrust policy p2 then reject
profile profile1
```

Results

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

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

from-zone trust to-zone untrust {
    policy p2 {
        match {
```

```
            source-address any;
            destination-address any;
            application junos-defaults;
            dynamic-application [ junos:GMAIL, junos:FACEBOOK-CHAT ];
            url-category Enhanced_News_and_Media;
        }
        then {
            reject {
                profile profile1;
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

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

```
user@host> show security policies

Default policy: permit-all
Pre ID default policy: permit-all
```

```
From zone: untrust, To zone: internet
  Policy: ip1, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-ping, junos-pingv6, junos-dns-udp, junos-dns-tcp
    Action: permit, log
  Policy: ip2, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: junos-ping, junos-pingv6, junos-telnet, junos-dns-udp, junos-dns-tcp, junos-
ftp, junos-http, junos-https
    Action: permit, log
From zone: untrust, To zone: trust
  Policy: up3, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: H1, H1_v6
    Destination addresses: H0, H0_v6
    Applications: junos-ping, junos-telnet, junos-ftp, junos-http, junos-https, my_app_udp,
my_app_tcp
    Dynamic Applications: junos:HTTP, junos:GOOGLE-GEN, junos:YAHOO, junos:SSL
    Url-category: Enhanced_Search_Engines_and_Portals, cust_white
    Action: permit, log
  Policy: up4, State: enabled, Index: 9, Scope Policy: 0, Sequence number: 2
    Source addresses: as1
    Destination addresses: as0
    Applications: junos-ping, junos-telnet, junos-ftp, junos-http, junos-https, my_app_udp,
my_app_tcp
    Dynamic Applications: junos:web, junos:FTP
    Url-category: Enhanced_Private_IP_Addresses, cust_white
    Action: permit, log
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses
- Configured applications
- Configured dynamic applications
- Configured URL Category

- Policy reject action

Configure Applications in Unified Policies

IN THIS SECTION

Applications in Unified Policies

Starting in Junos OS Release 19.1R1, configuring the `application` statement at the `[edit security policies from-zone` *`zone-name`* `to-zone` *`zone-name`* `policy` *`policy-name`* `match]` hierarchy level is optional if the `dynamic-application` statement is configured at the same hierarchy level.

In releases before Junos OS Release 19.1R1, it is mandatory to configure the `application` statement even if the `dynamic-application` statement is configured.

- When the `application` option is defined then the defined application is used.
- When the `application` option is not defined and the `dynamic-application` option is defined as `any`, then the application `any` is implicitly added.
- When the `application` option is not defined and the `dynamic-application` option is defined (and is not configured as `any`), then the application `junos-defaults` is implicitly added.

Example: Configure a Unified Policy Using Dynamic Applications

IN THIS SECTION

This example describes how to configure a unified policy using dynamic applications.

Requirements

This example uses the following hardware and software components:

- SRX Firewall running Junos OS Release 19.1R1. This configuration example is tested with Junos OS release 19.1R1.

Before you begin, configure security zones. See "Example: Creating Security Zones" on page 9.

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

Overview

In this example, dynamic applications are added to the security policy as match criteria.

To accomplish these objectives, perform the following tasks:

- Configure the security policy match criteria `source-address` and `destination-address` with the value `any`.
- Configure `dynamic-application` with `[junos:CNN, junos:BBC]` so that the policy can permit the applications junos:CNN and junos:BBC.

Configuration

IN THIS SECTION

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

CLI Quick Configuration

```
set security zones security-zone trust
set security zones security-zone untrust
```

```
set security policies from-zone trust to-zone untrust policy p3 match source-address any
set security policies from-zone trust to-zone untrust policy p3 match destination-address any
set security policies from-zone trust to-zone untrust policy p3 match dynamic-application
junos:CNN
set security policies from-zone trust to-zone untrust policy p3 match dynamic-application
junos:BBC
set security policies from-zone trust to-zone untrust policy p3 then permit
```

Step-by-Step Procedure

Step-by-Step Procedure

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

To configure a unified policy using dynamic applications:

1. Configure security zones.

```
[edit security]
user@host# set security-zone trust
user@host# set security-zone untrust
```

2. Create a security policy with a dynamic application as the match criteria.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p3 match source-address any
user@host# set from-zone trust to-zone untrust policy p3 match destination-address any
user@host# set from-zone trust to-zone untrust policy p3 match dynamic-application junos:CNN
user@host# set from-zone trust to-zone untrust policy p3 match dynamic-application junos:BBC
```

3. Define the policy action.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p3 then permit
```

Results

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

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

from-zone trust to-zone untrust {
    policy p3 {
        match {
            source-address any;
            destination-address any;
            dynamic-application [ junos:CNN junos:BBC ];
        }
        then {
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Unified Policy Configuration

Purpose

Verify that the unified policy configuration is correct.

Action

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

```
user@host> show security policies

  Policy: p3, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:CNN, junos:BBC
    Action: permit
```

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

```
user@host> show security policies detail

Default policy: permit-all
Pre ID default policy: permit-all
Policy: p3, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: TCP, ALG: 0, Inactivity timeout: 1800
      Destination ports: 80, 443, 3128, 8000, 8080
  Dynamic Application:
    junos:BBC: 1754
    junos:CNN: 988
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

Meaning

The output displays information about all currently active security sessions on the device. Verify the following information:

- Configured policy name
- Source and destination addresses
- Configured applications

> **NOTE**: The `Applications` field is autopopulated and its value `junos-defaults` is added implicitly.

- Configured dynamic applications
- Policy action

SEE ALSO

dynamic-application (Security Policies)

Configure Micro-Applications in Unified Policies

IN THIS SECTION

Starting in Junos OS Release 19.2R1, you can configure micro-applications in a unified policy. Micro-applications are sub-functions of an application. Micro-applications enable granular control of an application at a sub-function level instead of blocking or allowing the entire application. By default, detection of micro-applications is disabled.

The application identification (AppID) module detects an application at a sub-function level on your network. Security policies leverage the application identity information determined by the AppID module. After a specific application is identified, an action such as permit, deny, reject, or redirect is applied to the traffic according to the policy configured on the device. You must enable detection of micro-applications to use them in a security policy. See *Enabling and Disabling Micro-Applications Detection*.

Limit the Number of Policy Lookups

To process a policy, the policy lookup must return the *final match* state for the application. When using a micro-application, application classification does not reach the *final match* state because the micro-application constantly changes for the session. Because the micro-application changes from one transaction to another, an unlimited number of policy lookups is attempted.

Use the `unified-policy max-lookups` statement at the `[edit security policies]` hierarchy level to limit the number of policy lookups.

Configure Micro-Applications

To permit a base-level application and all its dependent micro-applications, you can configure a unified policy by specifying the base-level application as a matching criterion. You do not have to explicitly specify each dependent application as matching criteria for the policy. For example, if you specify the base-level application **junos-MODBUS** as a matching criterion in a unified policy, then you don't have to configure the micro-applications of the **junos-MODBUS** application (**junos:MODBUS-READ-COILS** and **junos:MODBUS-WRITE-SINGLE-COIL**) as matching criteria for the policy.

If you want to define a unified policy for granular-level control, then you must specify the micro-applications of the base-level application as matching criteria for the policy. You must not define the base-level application as match criteria in the policy. For more granular-level policy configuration, specify **junos:MODBUS-READ-COILS** as matching criteria in a unified policy. Ensure that the base-level application **junos:MODBUS** is not defined as as a matching criterion in the same unified policy.

Policy Lookup with Micro-Applications

Detection of micro-applications is disabled by default. To use micro-applications as matching criteria for policy lookup, you must enable detection of micro-applications and then specify them as matching criteria for the unified policy. If you have not enabled detection of micro-applications, the application identification (AppID) module does not detect any micro-application and considers the base-level application as the final matching criterion. For example, consider the base-level application **junos-:MODBUS** that has two micro-applications **junos:MODBUS-READ-COILS** and **junos:MODBUS-WRITE-SINGLE-COIL**:

- If you have not enabled detection of micro-applications, **junos:MODBUS** is considered as the *final match* state for the AppID classification. If you enable micro-applications, then you can configure them in a unified policy as any other pre-defined dynamic application. This micro-application is used for policy lookup.

- If you have enabled detection of micro-applications, the AppID module considers **junos:MODBUS** as the *pre-match* state. When the AppID module detects either **junos:MODBUS-READ-COILS** or **junos:MODBUS-WRITE-SINGLE-COIL**, AppID considers this result as the *final match* state and proceeds with policy lookup using this matching criterion.

SEE ALSO

Application Identification Support for Micro-Applications

max-lookups

Dynamic Application Classification States

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
change-completed	
change-completed	

RELATED DOCUMENTATION

Unified Policies Support for Flow

Understanding Unified Policies [Unified Threat Management (UTM)]

Overview of IDP Policy support for Unified Policies

Global Security Policies

IN THIS SECTION

A security policy is a stateful firewall policy and controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specific IP sources to specific IP destinations at scheduled times. To avoid creating multiple policies across every possible context, you can create a global policy that encompasses all zones, or a multizone policy that encompasses several zones. Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address and also provides access to multiple source zones and multiple destination zones in one policy.

Global Policy Overview

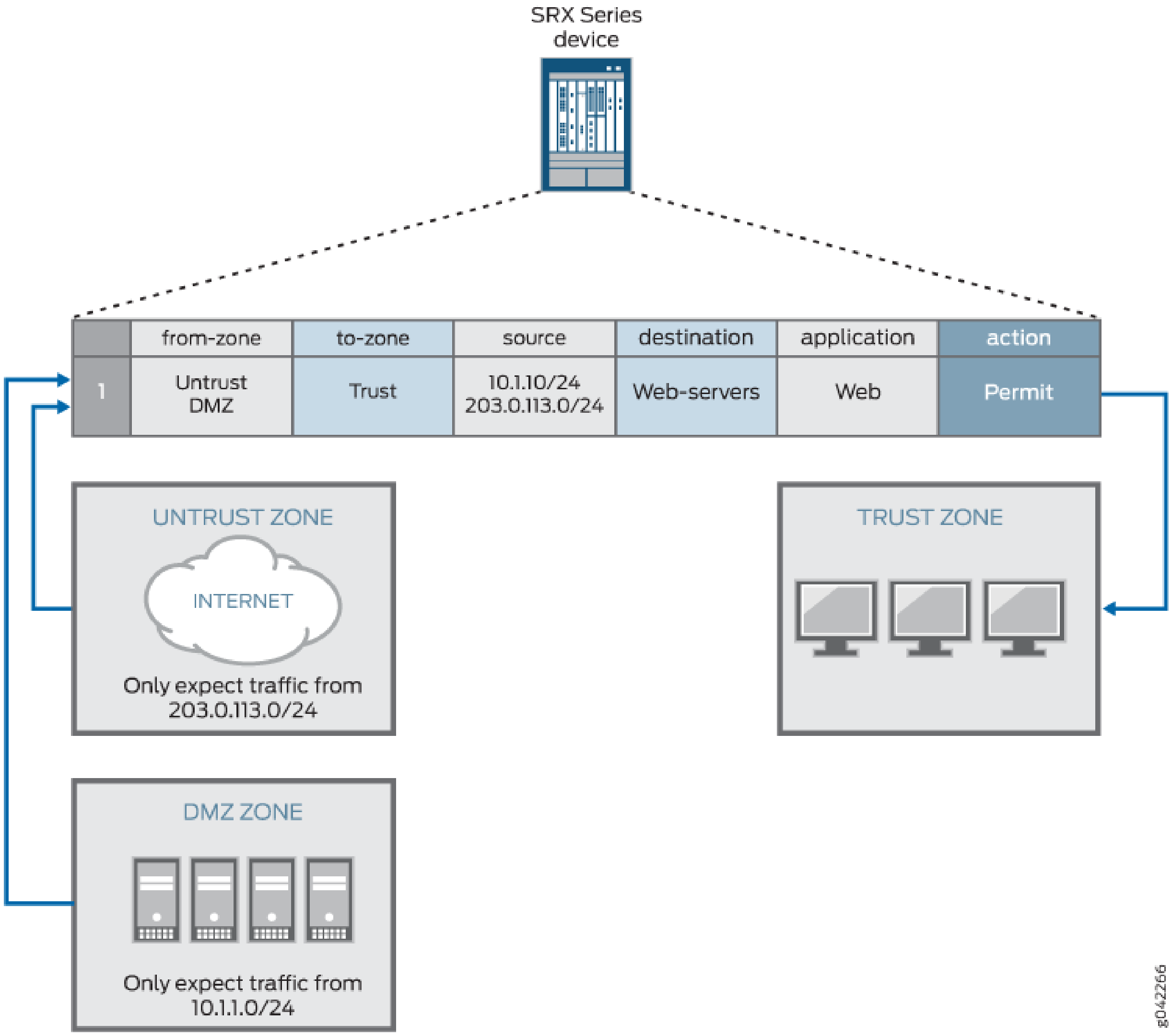
In a Junos OS stateful firewall, security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. Security policies require traffic to enter one security zone and exit another security zone. This combination of a from-zone and to-zone is called a *context*. Each context contains an ordered list of policies. Each policy is processed in the order that it is defined within a context. Traffic is classified by matching the policy's from-zone, to-zone, source address, destination address, and the application that the traffic carries in its protocol header. Each global policy, as with any other security policy, has the following actions: permit, deny, reject, log, count.

You can configure a security policy from the user interface. Security policies control traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specific IP sources to specific IP destinations at scheduled times. This works well in most cases, but it is not flexible enough. For example, if you want to perform actions on traffic you have to configure policies for each possible context. To avoid creating multiple policies across every possible context, you can create a global policy that encompasses all zones, or a multizone policy that encompasses several zones.

Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address "any." These addresses can span multiple security zones. For example, if you want to provide access to or from multiple zones, you can create a global policy with the address "any," which encompasses all addresses in all zones. Selecting the "any" address matches any IP address, and when "any" is used as a source/destination address in any global policy configuration, it matches the source/destination address of any packet.

Using a global policy you can also provide access to multiple source zones and multiple destination zones in one policy. However, we recommend that, for security reasons and to avoid spoofing traffic, when you create a multizone policy you use identical matching criteria (source address, destination address, application) and an identical action. In Figure 9 on page 185, for example, if you create a multizone policy that includes DMZ and Untrust from-zones, spoofing traffic from 203.0.113.0/24 from the DMZ zone could match the policy successfully and reach the protected host in the Trust to-zone.

Figure 9: Multizone Global Policy Security Consideration



NOTE: Global policies without from-zone and to-zone information do not support VPN tunnels because VPN tunnels require specific zone information.

When policy lookup is performed, policies are checked in the following order: intra-zone (trust-to-trust), inter-zone (trust-to-untrust), then global. Similar to regular policies, global policies in a context are ordered, such that the first matched policy is applied to the traffic.

NOTE: If you have a global policy, make sure you have not defined a "catch-all" rule such as, match source any, match destination any, or match application any in the intra-zone or inter-zone policies because the global policies will not be checked. If you do not have a global policy, then it is recommended that you include a "deny all" action in your intra-zone or inter-zone policies. If you do have a global policy, then you should include a "deny all" action in the global policy.

In logical systems, you can define global policies for each logical system. Global policies in one logical system are in a separate context than other security policies, and have a lower priority than regular security policies in a policy lookup. For example, if a policy lookup is performed, regular security policies have priority over global policies. Therefore, in a policy lookup, regular security policies are searched first and if there is no match, global policy lookup is performed.

SEE ALSO

Security Policies Overview | 2

Understanding Security Policy Rules | 97

Understanding Security Policy Elements | 96

Example: Configuring a Global Policy with No Zone Restrictions

IN THIS SECTION

Unlike other security policies in Junos OS, global policies do not reference specific source and destination zones. Global policies reference the predefined address "any" or user-defined addresses that can span multiple security zones. Global policies give you the flexibility of performing actions on traffic without any zone restrictions. For example, you can create a global policy so that every host in every zone can access the company website, for example, www.example.com. Using a global policy is a convenient shortcut when there are many security zones. Traffic is classified by matching its source address, destination address, and the application that the traffic carries in its protocol header.

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

Requirements

Before you begin:

- Review the firewall security policies.

  See "Security Policies Overview" on page 2, "Global Policy Overview" on page 184, "Understanding Security Policy Rules" on page 97, and"Understanding Security Policy Elements" on page 96.

- Configure an address book and create addresses for use in the policy.

  See "Example: Configuring Address Books and Address Sets" on page 36.

- Create an application (or application set) that indicates that the policy applies to traffic of that type.

  See "Example: Configuring Security Policy Applications and Application Sets" on page 56.

Overview

IN THIS SECTION

This configuration example shows how to configure a global policy that accomplishes what multiple security policies (using zones) would have accomplished. Global policy gp1 permits all traffic while policy gp2 denies all traffic.

Topology

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 security address-book global address server1 dns-name www.example.com
set security address-book global address server2 dns-name www.mail.example.com
set security policies global policy gp1 match source-address server1
set security policies global policy gp1 match destination-address server2
set security policies global policy gp1 match application any
set security policies global policy gp1 then permit
set security policies global policy gp2 match source-address server2
set security policies global policy gp2 match destination-address server1
set security policies global policy gp2 match application junos-ftp
set security policies global policy gp2 then deny
```

Procedure

Step-by-Step Procedure

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

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

1. Create addresses.

```
[edit security]
user@host# set security address-book global address server1 dns-name www.example.com
user@host# set security address-book global address server2 dns-name www.mail.example.com
```

2. Create the global policy to permit all traffic.

```
[edit security]
user@host# set policy global policy gp1 match source-address server1
user@host# set policy global policy gp1 match destination-address server2
user@host# set policy global policy gp1 match application any
user@host# set policy global policy gp1 then permit
```

3. Create the global policy to deny all traffic.

```
[edit security]
user@host# set policy global policy gp2 match source-address server2
user@host# set policy global policy gp2 match destination-address server1
user@host# set policy global policy gp2 match application junos-ftp
user@host# set policy global policy gp2 then deny
```

Results

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

```
user@host# show security policies
global {
    policy gp1 {
        match {
            source-address server1;
            destination-address server2;
            application any;
        }
        then {
            permit;
        }
    }
    policy gp2 {
        match {
            source-address server2;
            destination-address server1;
            application junos-ftp;
```

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

```
user@host# show security policies global
policy gp1 {
    match {
        source-address server1;
        destination-address server2;
        application any;
    }
    then {
        permit;
    }
}
policy gp2 {
    match {
        source-address server2;
        destination-address server1;
        application junos-ftp;
    }
    then {
        deny;
    }
}
```

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

Verification

IN THIS SECTION

Verifying Global Policy Configuration

Purpose

Verify that global policies gp1 and gp2 are configured as required.

Action

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

```
user@host> show security policies global

Global policies:
  Policy: gp1, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: server1
    Destination addresses: server2
    Applications: any
    Action: permit
  Policy: gp2, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 2
    From zones: any
    To zones: any
    Source addresses: server2
    Destination addresses: server1
    Applications: junos-ftp
    Action: deny
```

Meaning

The output displays information about all the global policies configured on the device.

Example: Configuring a Global Policy with Multiple Zones

IN THIS SECTION

Unlike other security policies in Junos OS, global policies allow you to create multizone policies. A global policy is a convenient shortcut when there are many security zones, because it enables you to configure multiple source zones and multiple destination zones in one global policy instead of having to create a separate policy for each from-zone/to-zone pair, even when other attributes, such as source-address or destination-address, are identical.

Requirements

Before you begin:

- Review the firewall security policies.

  See "Security Policies Overview" on page 2, "Global Policy Overview" on page 184, "Understanding Security Policy Rules" on page 97, and "Understanding Security Policy Elements" on page 96.

- Create security zones.

  See "Example: Creating Security Zones" on page 9

Overview

IN THIS SECTION

This configuration example shows how to configure a global policy that accomplishes what multiple security policies would have accomplished. Global policy Pa permits all traffic from zones 1 and 2 to zones 3 and 4.

Topology

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 security policies global policy Pa match source-address any
set security policies global policy Pa match destination-address any
set security policies global policy Pa match application any
set security policies global policy Pa match from-zone zone1
set security policies global policy Pa match from-zone zone2
set security policies global policy Pa match to-zone zone3
set security policies global policy Pa match to-zone zone4
set security policies global policy Pa then permit
```

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*.

To configure a global policy with multiple zones:

1. Create a global policy to allow any traffic from zones 1 and 2 to zones 3 and 4.

```
[edit security]
set security policies global policy Pa match source-address any
set security policies global policy Pa match destination-address any
set security policies global policy Pa match application any
set security policies global policy Pa match from-zone zone1
set security policies global policy Pa match from-zone zone2
set security policies global policy Pa match to-zone zone3
set security policies global policy Pa match to-zone zone4
set security policies global policy Pa then permit
```

Results

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

```
[edit]
user@host# show security policies global
policy Pa {
    match {
        source-address any;
        destination-address any;
        application any;
        from-zone [ zone1 zone2 ];
        to-zone [ zone3 zone4 ];
    }
    then {
        permit;
    }
}
```

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

Verification

IN THIS SECTION

Verifying Global Policy Configuration

Purpose

Verify that the global policy is configured as required.

Action

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

RELATED DOCUMENTATION

Security Policies Overview | 2

Configuring Security Policies | 96

User Role Firewall Security Policies

IN THIS SECTION

User role firewall policies allows the administrators to permit or restrict network access for users based on the roles they are assigned. User role firewalls enable greater threat mitigation, provide more informative forensic resources, improve record archiving for regulatory compliance, and enhance routine access provisioning.

Understanding User Role Firewalls

Network security enforcement, monitoring, and reporting based solely on IP information soon will not be sufficient for today's dynamic and mobile workforce. By integrating user firewall policies, administrators can permit or restrict network access of employees, contractors, partners, and other users based on the roles they are assigned. User role firewalls enable greater threat mitigation, provide more informative forensic resources, improve record archiving for regulatory compliance, and enhance routine access provisioning.

User role firewalls trigger two actions:

- Retrieve user and role information associated with the traffic
- Determine the action to take based on six match criteria within the context of the zone pair

The source-identity field distinguishes a user role firewall from other types of firewalls. If the source identity is specified in any policy for a particular zone pair, it is a user role firewall. The user and role information must be retrieved before policy lookup occurs. If the source identity is not specified in any policy, user and role lookup is not required.

To retrieve user and role information, authentication tables are searched for an entry with an IP address corresponding to the traffic. If an entry is found, the user is classified as an authenticated user. If not found, the user is classified as an unauthenticated user.

The username and roles associated with an authenticated user are retrieved for policy matching. Both the authentication classification and the retrieved user and role information are used to match the source-identity field.

Characteristics of the traffic are matched to the policy specifications. Within the zone context, the first policy that matches the user or role and the five standard match criteria determines the action to be applied to the traffic.

The following sections describe the interaction of user and role retrieval and the policy lookup process, methods for acquiring user and role assignments, techniques for configuring user role firewall policies, and an example of configuring user role firewall policies.

User Role Retrieval and the Policy Lookup Process

For policy lookup, firewall policies are grouped by zone pair (the from zone and to zone). Within the context of the zone pair, IP-based firewall policies are matched to traffic based on five criteria—source IP, source port, destination IP, destination port, and protocol.

User role firewall policies include a sixth match criteria—source identity. The source-identity field specifies the users and roles to which the policy applies. When the source-identity field is specified in any policy within the zone pair, user and role information must be retrieved before policy lookup can proceed. (If all policies in the zone pair are set to `any` or have no entry in the source-identity field, user and role information is not required and the five standard match criteria are used for policy lookup.)

The user identification table (UIT) provides user and role information for an active user who has already been authenticated. Each entry in the table maps an IP address to an authenticated user and any roles associated with that user.

When traffic requires user and role data, each registered UIT is searched for an entry with the same IP address. If a user has not been authenticated, there is no entry for that IP address in the table. If no UIT entry exists, the user is considered an unauthenticated user.

Policy lookup resumes after the user and role information has been retrieved. The characteristics of the traffic are matched against the match criteria in the policies. The source-identity field of a policy can specify one or more users or roles, and the following keywords:

authenticated-user	Users that have been authenticated.
unauthenticated-user	Users that have not been authenticated.
any	All users regardless of authentication. If the source-identity field is not configured or is set to any in all of the policies for the zone pair, only five criteria are matched.
unknown-user	Users unable to be authenticated due to an authentication server disconnection, such as a power outage.

For example, consider user-c who is assigned to the mgmt role. When traffic from the trust zone to the untrust zone is received from user-c at IP address 198.51.100.3, policy lookup is initiated. Table 21 on page 198 represents three policies in a user role firewall for the trust to untrust zone pair.

Table 21: Trust Zone to Untrust Zone Policy Sequence

src-zone	src-zone	dest-zone	src-IP	dest-IP	source-identity	Application	Action	Services
P1	trust	untrust	192.0.2.0	203.0.113.0	any	http	deny	–
P2	trust	untrust	any	any	mgmt	any	permit	–
P3	trust	untrust	198.51.100.3	any	employee	http	deny	–

All policies for the zone pair are checked first for a source-identity option. If any of the policies specifies a user, a role, or a keyword, user and role retrieval must occur before policy lookup continues. Table 21 on page 198 shows that policy P2 specifies mgmt as the source identity, making this a user role firewall. User and roles must be retrieved before policy lookup can continue.

NOTE: User and role retrieval would not be performed if the keyword any or if no source identity was specified in all of the policies in the zone context. In such cases, only the five remaining values are matched to the policy criteria.

The UIT represented in Table 22 on page 198 is checked for the IP address. Because the address is found, the username user-c, all roles listed for user-c (in this case, mgmt and employee), and the keyword authenticated-user become data used to match the traffic to the `source-identity` field of a policy.

Table 22: UIT Authentication Details

Source IP Address	Username	Roles
192.0.2.4	user-a	employee
198.51.100.3	user-c	mgmt, employee
203.0.113.2	user-s	contractor

Policy lookup resumes and compares the match criteria in each policy in Table 21 on page 198 to the incoming traffic. Assuming all other criteria match, the first policy that specifies user-c, mgmt, employee, authenticated-user, or any in the source-identity field could be a match for this traffic. Policy P1 matches one of the retrieved roles for user-c, but the source IP address does not match; therefore policy lookup continues. For policy P2, all criteria match the traffic; therefore the policy action is followed and the traffic is permitted. Note that the traffic also matches policy P3, but user firewall policies are terminal—policy lookup ends when the first policy match is found. Because policy P2 matches all criteria, policy lookup ends and policy P3 is not checked.

Policies can also be based on the classification assigned to a user from the user and role retrieval results. Consider a different set of policies for the same zone pair represented by Table 23 on page 199. If traffic is received from user-q at IP 198.51.100.5, user and role retrieval is required because the source-identity field is specified in at least one of the policies.

Table 23: Trust Zone to Untrust Zone Policy Sequence

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	trust	untrust	any	any	un-authenticated-user	http	deny	–
P2	trust	untrust	any	any	mgmt	any	permit	–
P3	trust	untrust	198.51.100.3	any	employee	http	deny	–

When the UIT entries in Table 22 on page 198 are checked, no entry is found for IP address 198.51.100.5. Therefore, the user is considered an unauthenticated user. When policy lookup resumes, the traffic matches policy P1 and the traffic is denied.

Understanding the User Identification Table

IN THIS SECTION

On the SRX Series Firewall, the user identification table (UIT) contains the IP address, username, and role information for each authenticated user. Entries are ordered by IP address. When username and role information is required by a security policy, all UITs are checked. Finding the IP address in an entry in one of the UITs means that the user at that address has already been successfully authenticated.

Each authentication source maintains its own UIT independently and provides query functions for accessing data. Three types of UITs are supported—the local authentication table, the Unified Access Control (UAC) authentication table, and the firewall authentication table.

Local authentication table

A static UIT created on the SRX Series Firewall either manually or programmatically using CLI commands. All users included in the local authentication table are considered authenticated users. When a matching IP address is found, user and role information is retrieved from the table entry and associated with the traffic. User and role information can be created on the device manually or ported from a third-party authentication server, but the data in the local authentication table is not updated in real time.

UAC authentication table

A dynamic UIT pushed from the Junos Pulse Access Control Service to the SRX Series Firewall. The UAC authentication table of a Junos Pulse Access Control Service contains an entry for each authenticated user. The data in this table is updated and pushed to the SRX Series Firewall whenever its authentication table is updated. Depending on the device configuration, authentication could occur on the Junos Pulse Access Control Service itself or on a third-party authentication server. If the Access Control Service is relaying data from a third-party server, the data is restructured by the Access Control Service to match the file format of its authentication table and pushed to the SRX Series Firewall.

Firewall authentication table

A dynamic UIT created on the SRX Series Firewall when `user-firewall` is specified as the firewall authentication type in a security policy. This UIT provides an alternative user role source to UAC when firewall authentication is already in use on your SRX Series Firewall. In this way, users defined for pass-through authentication can also be used as a source for usernames and roles when the `user-firewall` option is specified as the firewall authentication type in a policy.

The `user-firewall` authentication type initiates firewall authentication to verify the user by using either local authentication information or external authentication servers supporting RADIUS, LDAP, or SecureID authentication methods. When this type is specified for firewall authentication, the username and associated groups (roles) from the authentication source are mapped to the IP address and added to the firewall authentication UIT.

Local Authentication Table

The local authentication table is managed with CLI commands that insert or delete entries. A local authentication table can be used as a backup solution when a dynamic UIT is not available, or to assign user and role information to devices that cannot authenticate to the network, such as printers or file servers. The local authentication table can be used for testing or to demonstrate how a user role firewall works without firewall authentication or the Access Control Service configured.

The IP addresses, user names, and roles from a third-party authentication source can be downloaded and added to the local authentication table programmatically using CLI commands. If an authentication source defines users and groups, the groups can be configured as roles and associated with the user as usual.

To be compliant with the UAC authentication table, user names are limited to 65 characters and role names are limited to 64 characters. The local authentication table has a maximum of 10,240 authentication entries on SRX1500 devices and above, 5120 authentication entries on SRX650 devices and below, depending on the Junos OS release in your installation. The local authentication table has 5120 authentication entries on the vSRX Virtual Firewall. Each authentication entry can be associated with up to 200 roles. The maximum capacity is based on an average of 10 roles assigned to each user. This is the same capacity specified for a UAC authentication table.

Use the following command to add an entry to a local authentication table. Note that each entry is keyed by IP address.

```
user@host> request security user-identification local-authentication-table add user user-name ip-
address ip-address role [role-name role-name ]
```

The role option in a single CLI command accepts up to 40 roles. To associate more than 40 roles with a single user, you need to enter multiple commands. Keep the following characteristics in mind when adding or modifying authentication user and role entries.

- Role names cannot be the same as usernames.
- Using the `add` option with an existing IP address and username aggregates the role entries. The table can support up to 200 roles per user.
- Using the `add` option with an existing IP address and a new username overwrites the existing username for that IP address.
- Role aggregation does not affect existing sessions.
- To change the role list of an existing entry, you need to delete the existing entry and add an entry with the new role list.

- To change the IP address of an existing entry, you need to delete the existing entry and add an entry with the new IP address.

An entry can be deleted by IP address or by username.

```
user@host> request security user-identification local-authentication-table delete (ip-address |
user-name)
```

The local authentication table can be cleared with the following command:

```
user@host> clear security user-identification local-authentication-table
```

To display the content of the local authentication table, use the following `show...` command:

```
user@host> show security user-identification local-authentication-table all (brief | extensive)
```

The `brief` option (the default) displays information in a tabular format sequenced by IP address. User names and role lists are truncated to fit the format.

```
user@host> show security user-identification local-authentication-table all
```

```
Total entries: 2
Source IP       Username            Roles
198.51.100.1       user1            role1
203.0.113.2        user2            role2, role3
```

The `extensive` option displays the full content for each field. Other options limit the display to a single username, IP address, or role.

```
user@host> show security user-identification local-authentication-table all extensive
```

```
Total entries: 3
Ip-address: 198.51.100.2
Username: user1
Roles: role1

Ip-address: 203.0.113.2
```

```
Username: user1
Roles: role2

Ip-address: 192.0.2.3
Username: user3
Roles: role1, role2
```

UAC Authentication Table

An SRX Series Firewall can act as an enforcer for a Junos Pulse Access Control Service. In this implementation, the SRX Series Firewall acts as a Layer 3 enforcement point and controls access to resources with IP-based resource policies that have been pushed down from the Access Control Service.

When implemented as a user role firewall, the SRX Series Firewall can access the UAC network in a similar way for user role retrieval. In this instance, user and role information for all authenticated users is pushed from the Access Control Service.

The SRX Series Firewall configuration is similar to that of an enforcer. To establish communication, both devices require configuration and password settings to recognize the other. From the SRX Series Firewall, connect the Access Control Service as an infranet controller.

```
[edit]
user@host# set services unified-access-control infranet-controller ic-name address ip-address
user@host# set services unified-access-control infranet-controller ic-name interface interface-name
user@host# set services unified-access-control infranet-controller ic-name password password
```

From the Access Control Service, define the SRX Series Firewall as a New Enforcer. Use the same password specified on the SRX Series Firewall.

Users and passwords are defined on the Access Control Service as in a standard authentication configuration. One or more roles can also be associated with users. When a user is authenticated, an entry containing the IP address, username, and associated roles is added to the UAC authentication table on the Access Control Service.

The UAC authentication table is pushed from the Access Control Service to the SRX Series Firewall when the connection between the two devices is initialized. Whenever an entry is added, removed, or updated on the Access Control Service, the updated UAC authentication table is pushed to the SRX Series Firewall.

Resource access policies are not necessary on the Access Control Service for a user role firewall implementation. The access behavior is provided in the policy configurations on the SRX Series Firewall. If resource access policies are defined on the Access Control Service, they are pushed to the SRX Series

Firewall, but they are not used unless a specific firewall policy implements UAC policies in the policy's action field.

The following `show services` command displays the content of the UAC authentication table on the SRX Series Firewall, confirming that the table has been pushed from the Access Control Service successfully:

```
user@host> show services unified-access-control authentication-table extended
```

```
Id    Source IP       Username     Age   Role name
3     192.0.2.1          april        60    Users
6     192.0.2.2          june         60    Employeees
Total: 2
```

The SRX Series Firewall monitors connections and detects if communication to the Access Control Service has been lost. Based on the UAC configuration, the SRX Series Firewall waits for a response for a configured interval before issuing another request. If a response is received, the Access Control Service is considered functional. If no response is received after a specified timeout period, communication is considered lost and the timeout action is applied. The following UAC command syntax configures the interval, timeout, and timeout action:

```
user@host# set services unified-access-control interval seconds
user@host# set services unified-access-control timeout seconds
user@host# set services unified-access-control timeout-action (close | no-change | open)
```

During a disconnection, if user and role lookup is attempted for the disconnected device, it returns a failure code regardless of the timeout action. If access to all authentication sources is lost, the keyword unknown-user is associated with the IP address. When policy lookup resumes, a policy with unknown-user as the source identity would match the traffic. By implementing a specific policy for unknown-user, you can create a method for handling the loss of authentication sources.

Firewall Authentication Table

Firewall authentication requires users to authenticate to the SRX Series Firewall before permitting access between zones and devices. When traffic is received, the user is prompted for a username and password, and verified against a specified profile of valid users. Depending on the device configuration, firewall authentication verifies that telnet, HTTP, HTTPS (for SRX5800, SRX5600, and SRX5400 devices), and FTP traffic has been authenticated locally or by a RADIUS, LDAP, or SecureID authentication server.

If firewall authentication is in use on a device, the authentication process can also provide the username and role information needed for user role firewall match criteria. In this case, the information is collected and maintained in a UIT called the firewall authentication table. One or more access policies in the `edit access` hierarchy define authentication methods to be used for firewall authentication.

The firewall authentication table must be enabled as the authentication source for user role information retrieval. The `priority` option specifies the sequence in which all UITs will be checked.

```
user@host# set security user-identification authentication-source firewall-authentication
priority priority
```

In a firewall policy for a given zone pair, the `firewall-authentication` service specified for the `permit` action initiates authentication of matching traffic. The `user-firewall` authentication type generates the UIT entry for the authenticated user. The name specified in the `access-profile` option identifies the profile to be used to authenticate valid users.

```
[edit security policies from-zone zone to-zone zone policy policy-name]
user@host# set match source-identity unauthenticated-user
user@host# set then permit firewall-authentication user-firewall access-profile profile-name
```

The UIT table entry contains the IP address of the traffic mapped to the authenticated user and the user's associated groups. When the user is no longer active, the entry is removed from the table. Because entries are continuously added and removed as the traffic and authenticated users change, the firewall authentication table is considered dynamic.

When policies within the same zone pair specify the `source-identity` field as part of its match criteria, all enabled UITs are searched for an entry corresponding to the IP address of the traffic. If found, the associated username and groups are retrieved for source-identity matching. (User authentication group names are considered role names for source-identity matching.)

Policy Provisioning With Users and Roles

All users and roles, whether defined on the SRX Series Firewall or on the Access Control Service, are maintained in a user role file on the SRX Series Firewall. To display all users and roles available for provisioning, use the following `show security...` commands.

NOTE: Usernames and roles in the firewall authentication table are not included in the following displays.

- To display all of the roles that are available for provisioning, use the `show security user-identification role-provision all` command. Note that the roles from all UITs are listed together.
- To display all of the users that are available for provisioning, use the `show security user-identification user-provision all` command.
- To display all of the users and roles that are available for provisioning, use the `show security user-identification source-identity-provision all` command.

When a policy configuration is committed, the user role file is checked to determine if all users and roles specified in the policy are available for provisioning. If a user or role is not found, a warning identifies the missing user or role so that you can define it later.

NOTE: The policy is committed even if a user or role is not yet defined.

Obtaining Username and Role Information Through Firewall Authentication

User role firewall policies can be integrated with firewall authentication both to authenticate users and to retrieve username and role information. The information is mapped to the IP address of the traffic, stored in the firewall authentication table, and used for user role firewall policy enforcement.

The following CLI statements configure firewall authentication for user role firewall enforcement.

1. If not already established, define the access profile to be used for firewall authentication. You can skip this step if an existing access profile provides the client data needed for your implementation.

   The access profile is configured in the `[edit access profile]` hierarchy as with other firewall authentication types. It defines clients as firewall users and the passwords that provide them access. Use the following command to define a profile and add client names and passwords for firewall authentication.

   ```
   set access profile profile-name client client-name firewall-user password pwd
   ```

2. If HTTPS traffic is expected, define the access profile to be used for SSL termination services. You can skip this step if an existing SSL termination profile provides the services needed for your implementation.

The SSL termination profile is configured in the `[edit services ssl]` hierarchy.

```
set services ssl termination profile ssl-profile-name server-certificate certificate-type
```

3. Enable the firewall authentication table as an authentication source.

```
set security user-identification authentication-source firewall-authentication priority
priority
```

The priority value determines the sequence in which authentication sources are checked. The default value is 150 for the firewall authentication table. (It is 100 for the local authentication table and 200 for the Unified Access Control (UAC) authentication table.) By default, the local authentication table is checked first, the firewall authentication table is next, and the UAC authentication table is third if it is enabled. You can change this sequence by changing the priority value of one or more of the tables.

4. Configure policies that permit traffic for user firewall authentication.

```
edit security policies from-zone zone to-zone zone policy policy-name
set match source-identity unauthenticated-user
set then permit firewall-authentication user-firewall access-profile profile-name ssl-
termination-profile profile-name
```

When unauthenticated traffic is permitted for firewall authentication, the user is authenticated based on the access profile configured in this statement. The `ssl-termination-profile` option is needed only for HTTPS traffic.

By specifying the authentication type `user-firewall`, the firewall authentication table is propagated with the IP address, the username, and any group names associated with the authenticated user. (Group names from firewall authentication are interpreted as roles by the user role firewall.) Any further traffic from this IP address will match the IP address in the firewall authentication table, and not require authentication. The associated username and roles are retrieved from the table for use as potential match criteria in subsequent security policies.

Configuring a User Role Firewall For Captive Portal Redirection

To automatically redirect unauthenticated users to the Access Control Service, use the UAC captive portal feature. The following syntax defines the profile for the captive portal:

```
set services unified-access-control captive-portal profile-name redirect-traffic
[unauthenticated | all]
set services unified-access-control captive-portal profile-name redirect-url host-url
```

The Kerberos protocol, used for authentication encryption, identifies the Access Control Service only by its service principal name (SPN). The protocol does not accept an IP address. Therefore, the format for the redirect URL must be

```
service://hostname/options
```

In this implementation, the service is HTTP and the hostname is the FQDN of the Access Control Service. Options specified after the hostname pass additional information to the Access Control Service directing the user back to the original destination, to the SRX Series Firewall, or to the policy that originated the redirection. You can configure the options using the following keyword and variable pairs:

?target=%dest-url% Specifies the protected resource which the user is trying to access.

&enforcer=%enforcer-id% Specifies the ID assigned to the SRX Series Firewall when it is configured as an enforcer by the Access Control Service.

&policy=%policy-id% Specifies the encrypted policy ID for the security policy that redirected the traffic.

The following statements define the profile of the captive portal named auth-redirect. The captive-portal redirects unauthenticated users to the URL of the Access Control Service for authentication. After successful authentication, the traffic will be directed back to the SRX Series Firewall.

```
[edit]
user@host# set services unified-access-control captive-portal auth-redirect redirect-traffic
unauthenticated
user@host# set services unified-access-control captive-portal auth-redirect redirect-url "http://
ic6000.example.com/?target=%dest-url%&enforcer=%enforcer-id%&policy=%policy-id%"
```

A defined captive-portal profile is displayed as part of the UAC configuration.

```
[edit]
user@host#show services
```

```
unified-access-control {
    captive-portal auth-redirect {
        redirect-traffic unauthenticated;
        redirect-url "http://ic6000.example.com/?target=%dest-url%&enforcer=%enforcer-id%&policy=
%policy-id%";
    }
}
```

After the profile is defined, a policy can apply the captive portal as an application service when certain criteria is matched. Whenever a user role is unauthenticated, auth-redirect captive portal diverts the traffic from trust zone to untrust zone. The following example defines policy P1 to apply the auth-redirect captive portal profile to any HTTP traffic from the trust to untrust:

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy P1 match application http
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-identity
unauthenticated-user
user@host# set security policies from-zone trust to-zone untrust policy P1 then permit
application-services uac-policy captive-portal auth-redirect
```

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

IN THIS SECTION

The following example configures a user role firewall on an SRX Series Firewall. The firewall controls access from the trust zone to the untrust zone based on active, authenticated users or their associated roles. User role firewall policies establish the following restrictions:

- Only authenticated users are permitted from the trust zone to the untrust zone.

  Unauthenticated users are redirected to an Access Control Service for authentication.

- Traffic from IP 192.0.2.0 to IP 203.0.113.0 within the zone context is restricted. Only the traffic from users with the dev-abc, http-juniper-accessible, or ftp-accessible role is permitted. Permitted traffic is further evaluated by AppFW rules.

  - Permitted traffic identified as junos:FACEBOOK-ACCESS, junos:GOOGLE-TALK, or junos:MEEBO application traffic is denied.

  - Permitted traffic for any other application is permitted.

- All other traffic from the trust zone to the untrust zone is permitted.

Requirements

Before you begin, ensure that the SRX Series Firewall with Junos OS Release 12.1 or later is configured and initialized.

In this example, user and role information associated with the IP address of the traffic is provided by an Access Control Service. For instructions on configuring the Access Control Server, see Configure Active Directory as Identity Source.

Overview

Table 24 on page 210 outlines a firewall that meets the requirements for this example. The user role firewall consists of four policies.

Table 24: User Role Firewall Policies

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
user-role-fw1	trust	untrust	any	any	un-authenticated-user	http	permit	UAC captive portal

Table 24: User Role Firewall Policies *(Continued)*

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
user-role-fw2	trust	untrust	192.0.2.0	203.0.113.0	dev-abc http-juniper-accessible ftp-accessible	http	permit	AppFW ruleset RS1
user-role-fw3	trust	untrust	192.0.2.0	203.0.113.0	any	http	deny	
user-role-fw4	trust	untrust	any	any	any	http	permit	

Because the `source-identity` field is specified for at least one of the policies in this firewall, user and role information must be retrieved before policy lookup is conducted. The source IP of the traffic is compared to the items in the UIT. If the source IP address is found, the keyword `authenticated`, the username, and any roles associated with this user are stored for later use in policy lookup. If a matching entry for the IP address is not found in the UIT, the keyword `unauthenticated-user` is stored for policy lookup.

After retrieving the username, roles, and keywords, policy lookup begins. Characteristics of the incoming traffic are compared to each policy's match criteria. If a match is found, the action specified in that policy is taken.

A policy match is a terminal event, and no policies after the match are checked. Policy sequence influences the action to be taken for matching traffic. In this example, policies are applied in the following sequence:

user-role-fw1
: Applies the UAC captive portal service to matching HTTP traffic with the unauthenticated-user keyword, and redirects it to the Access Control Service for authentication. A UAC profile must also be configured to identify the captive portal specifications.

user-role-fw2
: Applies an AppFW rule set to any HTTP traffic from address 192.0.2.0 to address 203.0.113.0 that has a matching username or role. An application firewall must also be configured to define the rule set.

user-role-fw3	Denies all remaining HTTP traffic from address 192.0.2.0 to address 203.0.113.0 for this zone pair.
user-role-fw4	Permits all remaining HTTP traffic for this zone pair.

Configuration

IN THIS SECTION

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

Configuring Redirection For Unauthenticated Users

Step-by-Step Procedure

When an IP address is not listed in the UIT, the unauthenticated-user keyword is used in policy lookup. Instead of denying access to this traffic, a policy can redirect the traffic to a UAC captive portal for authentication.

> **NOTE**: It is important to position a redirection policy for unauthenticated-user before a policy for “any” user so that UAC authentication is not shadowed by a policy intended for authenticated users.

To configure redirection from the SRX Series Firewall to the Access Control Service:

1. From configuration mode, configure the UAC profile for the captive portal acs-device.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device redirect-traffic
unauthenticated-user
```

2. Configure the redirection URL for the Access Control Service or a default URL for the captive portal.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device redirect-url
“https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%”
```

This policy specifies the default target and enforcer variables to be used by the Access Control Service to direct the user back after authentication. This ensures that changes to system specifications will not affect configuration results.

NOTE: When variables, such as `?target=`, are included in the command line, you must enclose the URL and variables in quotation marks.

3. Configure a user role firewall policy that redirects HTTP traffic from zone trust to zone untrust if the source-identity is unauthenticated-user. The captive portal profile name is specified as the action to be taken for traffic matching this policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match
source-address any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match
destination-address any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match
application http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 match
source-identity unauthenticated-user
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw1 then
permit application-services uac-policy captive-portal acs-device
```

4. If you are done configuring the policies, commit the changes.

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

Results

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

```
[edit]
user@host# show services
unified-access-control {
    captive-portal acs-device {
        redirect-traffic unauthenticated;
        redirect-url “https://%ic-ip%/?target=%dest-url%&enforcer=%enforcer-id%”
```

```
user@host# show security policies
from-zone trust to-zone untrust {
    policy user-role-fw1 {
        match {
            source-address any;
            destination-address any;
            application http;
            source-identity unauthenticated-user
        }
        then {
            permit {
                application-services {
                    uac-policy {
                        captive-portal acs-device;
                    }
                }
            }
        }
    }
}
```

Creating a User Role Policy With an Application Firewall

Step-by-Step Procedure

This policy restricts traffic from IP192.0.2.0 to IP 203.0.113.0 based on its user and roles, and also its application. The configuration defines an application rule set and applies it to matching user role traffic.

1. Configure the AppFW rule set rs1. The following rule set denies junos:FACEBOOK-ACCESS, junos:GOOGLE-TALK, or junos:MEEBO application traffic. It applies the default setting, permit, to the remaining traffic.

```
[edit security application-firewall rule-sets rs1]
user@host# set rule r1 match dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLE-TALK
junos:MEEBO]
user@host# set rule r1 then deny
user@host# set default-rule permit
```

2. Configure a policy to apply the rs1 application firewall rule set to traffic from IP 192.0.2.0 to IP 203.0.113.0 with the dev-abc, http-mgmt-accessible, or ftp-accessible user role.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match
source-address 192.0.2.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match
destination-address 203.0.113.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match
application http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 match
source-identity [dev-abc http-mgmt-accessible ftp-accessible]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw2 then
permit application-services application-firewall rule-set rs1
```

3. If you are done configuring the policy, commit the changes.

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

Results

Verify that the AppFW rule set is configured properly. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security application-firewall
rule-sets rs1 {
        rule r1 {
```

```
            match {
                dynamic-application [junos:FACEBOOK-ACCESS junos:GOOGLE-TALK junos:MEEBO]
        }
            then {
                deny;
            }
        }
        default-rule {
            permit;
        }
}
```

Creating Remaining Security Policies Based on User and Role

Step-by-Step Procedure

The following procedure configures policies for the remaining traffic.

1. Configure a policy to deny traffic with the same source and destination address but with different user and role criteria than specified in the user-role-fw2 policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match
source-address 192.0.2.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match
destination-address 203.0.113.0
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match
application http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 match
source-identity any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw3 then
deny
```

2. Configure a security policy to permit all other HTTP traffic from zone trust to zone untrust.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match
source-address any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match
destination-address any
```

```
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match
application http
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 match
source-identity any
user@host# set security policies from-zone trust to-zone untrust policy user-role-fw4 then
permit
```

Results

Verify the content and sequence of the user role firewall policies. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show security policies
...
from-zone trust to-zone untrust {
    policy user-role-fw1 {
        match {
            source-address any;
            destination-address any;
            application http;
            source-identity unauthenticated-user
        }
        then {
            permit {
                application-services {
                    uac-policy {
                        captive-portal acs-device;
                    }
                }
            }
        }
    }
}
from-zone trust to-zone untrust {
        policy user-role-fw2 {
            match {
                source-address 192.0.2.0;
                destination-address 203.0.113.0;
                application http;
                source-identity [dev-abc http-juniper-accessible ftp-accessible]
```

```
            }
            then {
                permit {
                    application-services {
                        application-firewall {
                            rule-set rs1
                        }
                    }
                }
            }
        }
}
from-zone trust to-zone untrust {
        policy user-role-fw3 {
            match {
                source-address 192.0.2.0;
                destination-address 203.0.113.0;
                application http;
                source-identity any
            }
            then {
                deny
            }
        }
}
from-zone trust to-zone untrust {
    policy user-role-fw4 {
        match {
            source-address any;
            destination-address any;
            application http;
            source-identity any
        }
        then {
            permit
        }
    }
}
```

Configuring Resource Policies Using UAC

When using the user role firewall feature, resource policies are not necessary on the Access Control Service. If, however, resource policies exist, they are pushed to the SRX Series Firewall at connection. You can create policies that use these resource policies by applying the UAC application service in the policy configuration. Table 25 on page 219 shows three firewall policies that use the UAC resource policies exclusively:

Table 25: User Role Firewall Usage

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	zone1	zone2	any	192.0.2.1	any	http	permit	Content Security
P2	zone1	zone2	any	net2	any	http	permit	IDP
P3	zone1	zone2	any	any	any	any	permit	UAC

The policies for traffic from zone1 to zone2 do not initiate user and role retrieval because any is specified in the source-identity field of every policy. In this example, traffic to the IP address 192.0.2.1 is permitted, but must meet processing requirements for the specified application service, in this case, Content Security. Traffic to net2 is permitted and processed by the IDP processing requirements. Any remaining traffic is permitted and processed by the UAC processing requirements.

The configuration for this firewall policy would be as follows:

```
[edit]
user@host# show security policies
from-zone zone1 to-zone zone2 {
    policy P1 {
        match {
            source-address any;
            destination-address 192.0.2.1;
            source-identity any;
            application http;
        }
        then {
             permit {
```

```
                application-services {
                    idp;
                }
            }
        }
    }
}
from-zone zone1 to-zone zone2 {
    policy P2 {
        match {
            source-address any;
            destination-address net2;
            source-identity any;
            application http;
        }
        then {
             permit {
                application-services {
                    utm;
                }
            }
        }
    }
}
from-zone zone1 to-zone zone2 {
    policy P3 {
        match {
            source-address any;
            destination-address any;
            source-identity any;
            application any;
        }
        then {
             permit {
                application-services {
                    uac-policy;
                }
            }
        }
    }
}
```

In this sample configuration, the action fields in P1 and P2 apply any requirements that have been configured for IDP and Content Security respectively. By specifying the uac-policy option, the resource policies pushed to the SRX Series Firewall determine whether the destination is accessible.

A user role firewall can implement both user role policies and the resource policies pushed from the Access Control Service. Table 26 on page 221 shows the policies for three zone pairs.

Table 26: User Role Firewall Usage

policy-name	src-zone	dest-zone	src-IP	dest-IP	source-identity	application	action	Services
P1	zone1	zone2	any	any	unauthenticated-user	any	permit	UAC captive portal
P2	zone1	zone2	any	192.0.2.1	role2	http	permit	IDP
P3	zone1	zone2	any	net2	authenticated-user	http	permit	Content Security
P4	zone1	zone2	any	any	any	any	permit	
P5	zone1	zone3	any	any	any	any	permit	UAC
P6	zone2	zone3	any	any	any	any	permit	UAC

Traffic from zone1 to zone2 is subject to one of four user role policies. The first of these policies uses the UAC captive portal to redirect unauthenticated users to the Access Control Service for authentication.

The access of traffic from zone1 to zone3 and from zone2 to zone3 is controlled by the resource policies pushed from the Access Control Service.

Platform-Specific User Role Firewall Security Policies Behavior

IN THIS SECTION

Use Feature Explorer to confirm platform and release support for specific features.

Use the following tables to review platform-specific behavior for your platform:

Platform-Specific Local Authentication Behavior

Platform	Difference
SRX Series	• On SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 devices that support local authentication, the local authentication table has a maximum of 10,240 authentication entries depending on the Junos OS release in your installation.. • On SRX1500 and above devices that support this feature, the local authentication table has a maximum of 5120 authentication entries depending on the Junos OS release in your installation.

Platform-Specific Firewall Authentication Behavior

Platform	Difference
SRX Series	• On SRX5400, SRX5600, and SRX5800 devices that support firewall authentication, depending on the device configuration, firewall authentication verifies that telnet, HTTP, HTTPS and FTP traffic has been authenticated locally or by a RADIUS, LDAP, or SecureID authentication server.

RELATED DOCUMENTATION

Configuring Security Policies | 96

Monitoring and Troubleshooting Security Policies | 415

Reordering Security Policies

IN THIS SECTION

Reordering security policy allows to move the policies around after they have been created. Junos OS provides CLI statements and command for verifying that the order of policies in the policy list and change the order if required.

View and Change Security Policy Ordering

Security policies execute in the order of their appearance in the configuration file, you should be aware of the following:

- Policy order is important.
- New policies go to the end of the policy list.
- The last policy is the default policy, which has the default action of denying all traffic.

When you have configured the number of security policies, it is possible for one policy to eclipse, or *shadow*, another policy. In such case:

- You can view the list of shadowed policies in the policy list using the `show security shadow-policies` command.
- You can change the order of policies and put the more specific policy before other by using the `insert` and `before` statement.

Consider the following examples:

Example 1

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

Example 2

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/2.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic
system-services all
```

```
user@host# set security address-book book1 address mail-untrust 192.0.2.1/24
user@host# set security address-book book1 attach zone untrust
user@host# set security address-book book2 address mail-trust 192.168.1.1/24
user@host# set security address-book book2 attach zone trust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match source-
address mail-trust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match
destination-address mail-untrust
user@host# set security policies from-zone trust to-zone untrust policy permit-mail match
application junos-mail
user@host# set security policies from-zone trust to-zone untrust policy permit-mail then permit
```

In examples 1 and 2, where policy `permit-mail` is configured after policy `permit-all` from zone `trust` to zone `untrust`. All traffic coming from zone `untrust` matches the first policy `permit-all` and is allowed by default. No traffic matches policy `permit-mail`.

Because Junos OS performs a policy lookup starting from the top of the list, when it finds a match for traffic received, it does not look any lower in the policy list. To correct the previous example, you can simply reverse the order of the policies, putting the more specific one first:

```
[edit]
user@host# insert security policies from-zone trust to-zone untrust policy permit-mail before policy permit-
all
```

In cases where there are dozens or hundreds of policies, the eclipsing of one policy by another might not be so easy to detect. To check if policies are being shadowed, enter any of the following commands:

```
[edit]
user@host# run show security shadow-policies logical-system lsys-name from-zone from-zone-name to-zone to-
zone-name
```

```
[edit]
user@host# run show security shadow-policies logical-system lsys-name global
```

This command reports the shadowing and shadowed policies. It is then the administrator's responsibility to correct the situation.

NOTE: The concept of policy *shadowing* refers to the situation where a policy higher in the policy list always takes effect before a subsequent policy. Because the policy lookup always uses the first policy it finds that matches the five-part tuple of the source and destination zone, source and destination address, and application type, if another policy applies to the same tuple (or a subset of the tuple), the policy lookup uses the first policy in the list and never reaches the second one.

SEE ALSO

Security Policies Configuration Overview | **104**

Example: Configuring a Security Policy to Permit or Deny All Traffic | **107**

Example: Configuring a Security Policy to Permit or Deny Selected Traffic | **113**

RELATED DOCUMENTATION

Security Policies Overview | **2**

Scheduling Security Policies

IN THIS SECTION

Scheduler is a security feature that allows a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. You can create schedulers irrespective of a policy, meaning that a scheduler cannot be used by any policies.

Security Policy Schedulers Overview

Schedulers are powerful features that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. You can create schedulers irrespective of a policy, meaning that a scheduler cannot be used by any policies. However, if you want a policy to be active within a scheduled time, then you must first create a scheduler.

When a scheduler times out, the associated policy is deactivated. All sessions associated with the policy are subsequently timed out only if policy-rematch is used

If a policy contains a reference to a scheduler, the schedule determines when the policy is active, that is, when it can be used as a possible match for traffic. Schedulers allow you to restrict access to a resource for a period of time or remove a restriction.

The following guidelines apply to schedulers:

- A scheduler can have multiple policies associated with it; however, a policy cannot be associated with multiple schedulers.
- A policy is active during the time when the scheduler it refers to is also active.
- When a scheduler is off, the policy is unavailable for policy lookup.
- A scheduler can be configured as one of the following:
    - Scheduler can be active for a single time slot, as specified by a start date and time and a stop date and time.
    - Scheduler can be active forever (recurrent), but as specified by the daily schedule. The schedule on a specific day (time slot) takes priority over the daily schedule.
    - Scheduler can be active within a time slot as specified by the weekday schedule.
    - Scheduler can have a combination of two time slots (daily and timeslot).

Example: Configuring Schedulers for a Daily Schedule Excluding One Day

IN THIS SECTION

This example shows how to configure schedulers for packet match checks every day, from 8:00 AM to 5:00 PM, except Sunday.

Requirements

Before you begin:

- Understand security policies schedulers. See "Security Policies Overview" on page 2.
- Configure security zones before applying this configuration.

Overview

Schedulers are powerful features that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. If you want a policy to be active within a scheduled time, then you must first create a scheduler.

To configure a scheduler, you enter a meaningful name and a start and stop time for the scheduler. You can also attach comments.

In this example, you:

- Specify the scheduler, sch1, that allows a policy, which refers to it, to be used for packet match checks every day, from 8:00 AM to 5:00 PM, except Sunday.

  NOTE: Use the 24-hour format (hh:mm) to specify the hours and minutes for the daily time.

- Create a policy, abc, and specify the match conditions and action to be taken on traffic that matches the specified conditions. and bind the schedulers to the policy to allow access during the specified days.

Configuration

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.

```
set schedulers scheduler sch1 daily start-time 08:00 stop-time 17:00
set schedulers scheduler sch1 sunday exclude
set security policies from-zone green to-zone red policy abc match source-address any
set security policies from-zone green to-zone red policy abc match destination-address any
set security policies from-zone green to-zone red policy abc match application any
set security policies from-zone green to-zone red policy abc then permit
set security policies from-zone green to-zone red policy abc scheduler-name sch1
set security policies default-policy permit-all
```

Step-by-Step Procedure

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

To configure a scheduler:

1. Set a scheduler.

```
[edit schedulers ]
user@host# set scheduler sch1 daily start-time 08:00 stop-time 17:00
user@host# set scheduler sch1 sunday exclude
```

2. Specify the match conditions for the policy.

```
[edit security policies from-zone green to-zone red policy abc]
user@host# set match source-address any destination-address any application any
```

3. Specify the action.

```
[edit security policies from-zone green to-zone red policy abc]
user@host# set then permit
```

4. Associate the scheduler to the policy.

```
[edit security policies  from-zone green to-zone red policy abc ]
user@host# set scheduler-name sch1
```

Results

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

```
[edit]
[user@host]show schedulers
    scheduler sch1 {
        daily {
            start-time 08:00 stop-time 17:00;
        sunday exclude;
    }
[edit]
[user@host]show security policies
from-zone green to-zone red {
    policy abc {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
```

```
        }
        scheduler-name sch1;
    }
}
    default-policy {
        permit-all;
    }
```

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

Verification

IN THIS SECTION

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

Verifying Schedulers are Active

Purpose

Verify if schedulers are enabled or not.

Action

From operational mode, enter the `show schedulers` command.

Verifying Policies

Purpose

Verify if the policies are working.

Action

From operational mode, enter the `show security policies` command.

Verifying Scheduled Policies

IN THIS SECTION

Purpose

Display information about scheduled security policies.

Action

Use the `show schedulers` CLI command to display information about schedulers configured on the system. If a specific scheduler is identified, detailed information is displayed for that scheduler only.

```
user@host# show schedulers
scheduler sche1 {
    /* This is sched1 */
    start-date 2006-11-02.12:12 stop-date 2007-11-02.12:11;
}
scheduler sche2 {
    daily {
        all-day;
    }
    sunday {
        start-time 16:00 stop-time 17:00;
    }
    friday {
        exclude;
    }
}
scheduler sche3 {
    start-date 2006-11-02.12:12 stop-date 2007-11-02.12:11;
    daily {
        start-time 10:00 stop-time 17:00
```

```
    }
    sunday {
        start-time 12:00 stop-time 14:00;
        start-time 16:00 stop-time 17:00;
    }
    monday {
        all-day;
    }
    friday {
        exclude;
    }
}
```

Meaning

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

- Daily (recurrent) and one-time only (nonrecurrent) schedulers are configured correctly.
- Schedulers are active if policies are associated.

RELATED DOCUMENTATION

Configuring Security Policies | 96

Threat Profiling Support in Security Policy

SUMMARY

Read this topic to understand SRX Series Firewall support for threat feeds in the security policies.

IN THIS SECTION

Support for Threat Feeds in Security Policies

SRX Series Firewalls can generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events.

Juniper ATP Cloud service consolidates the generated feeds from SRX Series Firewall and shares the duplicated results back to the security device. The security device then uses the feeds to perform actions against the designated traffic. You can enable the security device to use the feeds by configuring security policies with the feeds as a matching criteria. When traffic matches policy conditions, the device applies policy actions.

SRX Series Firewalls support following types of threat feeds in the security policies:

- source and destination addresses
- user source identity (user name)

Workflow in using the threat feeds in security policies:

1. In a security policy, you can add the source address/destination address,/source identity (user name) as a feed for the policy action (deny, reject, and permit rules).
2. Policy module adds the username to the traffic's IP address into the feed.
3. Once the feed is created, Juniper ATP cloud consolidates feeds from all SRX Series Firewalls in your enterprise and sends result to SRX Series Firewall.
4. When you create another security policy, you can add the feed as match criteria.

See Adaptive Threat Profiling Overview for more information on configuring and deploying security policies with feeds.

Security Policies for VXLAN

SUMMARY

IN THIS SECTION

Configure Security Policies for VXLAN

SUMMARY

Use this example to configure security policies for EVPN (Ethernet VPN) Virtual Extensible LAN (VXLAN) tunnel inspection.

IN THIS SECTION

Requirements

VXLAN support on SRX Series Firewalls provides the flexibility to bring an enterprise grade firewall to connect end points in their campus, data center, branch and public cloud environments while providing embedded security.

This example uses the following hardware and software components:

- SRX4600 device
- Junos OS Release 20.4R1

Before you begin:

- Make sure you understand how EVPN and VXLAN works.

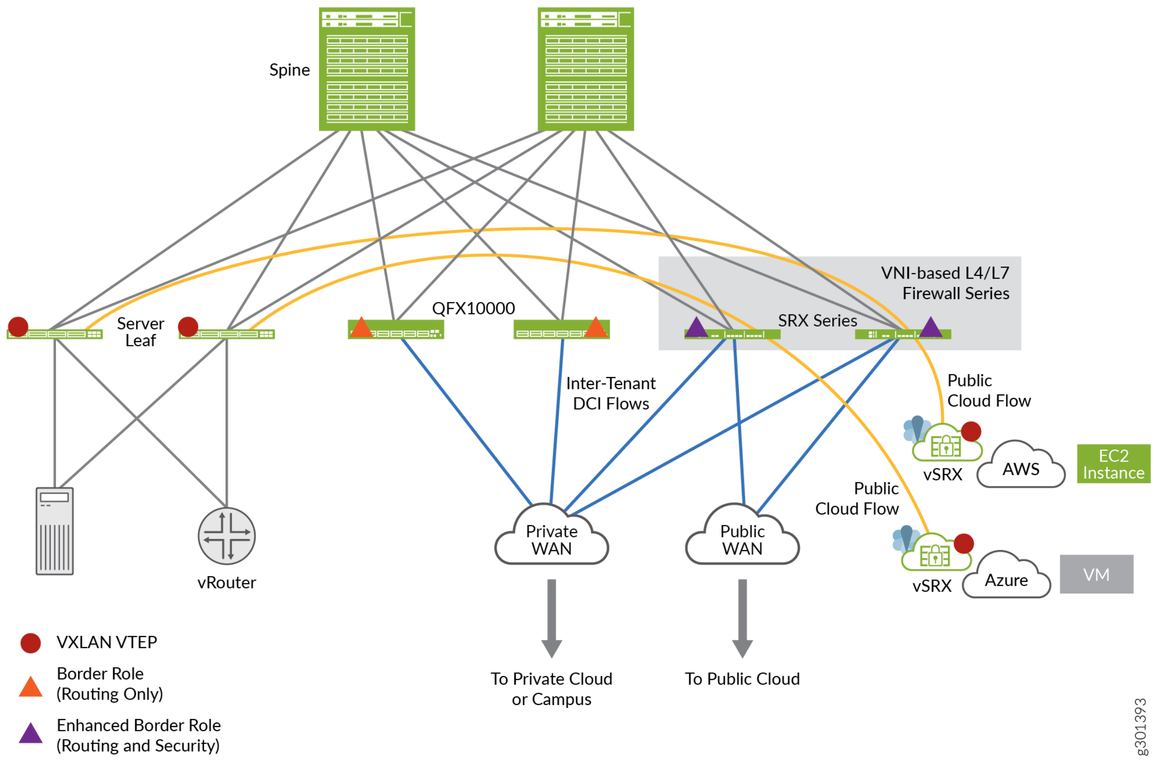
Overview

IN THIS SECTION

The EVPN solution provides large enterprises a common framework used to manage their campus and data center networks. An EVPN-VxLAN architecture supports efficient Layer 2 and Layer 3 network connectivity with scale, simplicity, and agility. Figure 10 on page 236 shows an simplified VXLAN traffic flow topology.

Topology

Figure 10: Simplified VXLAN Traffic Flow Topology



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 security zones security-zone cloud-1
set security zones security-zone dc
set security tunnel-inspection inspection-profile ins-pf1 vxlan vx1 vni r1
set security tunnel-inspection inspection-profile ins-pf1 vxlan vx1 vni r2
set security tunnel-inspection inspection-profile ins-pf1 vxlan vx1 vni r3
set security tunnel-inspection inspection-profile ins-pf1 vxlan vx1 vni r4
set security tunnel-inspection inspection-profile ins-pf1 vxlan vx1 policy-set pset1
set security tunnel-inspection vni r1 vni-range 160 to 200
set security tunnel-inspection vni r2 vni-id 155
set security tunnel-inspection vni r3 vni-range 300 to 399
set security tunnel-inspection vni r4 vni-range 100 to 120
set security tunnel-inspection vni v1 vni-range 1 to 100
set security policies from-zone dc to-zone cloud-1 policy p1 match source-address any
set security policies from-zone dc to-zone cloud-1 policy p1 match destination-address any
set security policies from-zone dc to-zone cloud-1 policy p1 match application junos-vxlan
set security policies from-zone dc to-zone cloud-1 policy p1 then permit tunnel-inspection ins-
pf1
set security policies from-zone cloud-1 to-zone dc policy p1 match source-address any
set security policies from-zone cloud-1 to-zone dc policy p1 match destination-address any
set security policies from-zone cloud-1 to-zone dc policy p1 match application junos-vxlan
set security policies from-zone cloud-1 to-zone dc policy p1 then permit tunnel-inspection ins-
pf1
set security policies policy-set pset1 policy pset_p1 match source-address any
set security policies policy-set pset1 policy pset_p1 match destination-address any
set security policies policy-set pset1 policy pset_p1 match application any
set security policies policy-set pset1 policy pset_p1 then permit
set security policies default-policy deny-all
```

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 VXLAN:

1. Define Security Zones.

```
[edit security zones]
user@host# set security-zone cloud-1
user@host# set zones security-zone dc
```

2. Define tunnel-inspection profile.

```
[edit security tunnel-inspection]
user@host# set inspection-profile ins-pf1 vxlan vx1 vni r1
user@host# set inspection-profile ins-pf1 vxlan vx1 vni r2
user@host# set inspection-profile ins-pf1 vxlan vx1 vni r3
user@host# set inspection-profile ins-pf1 vxlan vx1 vni r4
user@host# set inspection-profile ins-pf1 vxlan vx1 policy-set pset1
user@host# set vni r1 vni-range 160 to 200
user@host# set vni r2 vni-id 155
user@host# set vni r3 vni-range 300 to 399
user@host# set vni r4 vni-range 100 to 120
user@host# set vni v1 vni-range 1 to 100
```

3. Define outer session policies.

```
[edit security policies]
user@host# set from-zone dc to-zone cloud-1 policy p1 match source-address any
user@host# set from-zone dc to-zone cloud-1 policy p1 match destination-address any
user@host# set from-zone dc to-zone cloud-1 policy p1 match application junos-vxlan
user@host# set from-zone dc to-zone cloud-1 policy p1 then permit tunnel-inspection profile-1
user@host# set from-zone cloud-1 to-zone dc policy p1 match source-address any
user@host# set from-zone cloud-1 to-zone dc policy p1 match destination-address any
user@host# set from-zone cloud-1 to-zone dc policy p1 match application junos-vxlan
user@host# set from-zone cloud-1 to-zone dc policy p1 then permit tunnel-inspection ins-pf1
```

4. Define policy-set.

```
[edit security policies]
user@host# set policy-set pset1 policy pset_p1 match source-address any
user@host# set policy-set pset1 policy pset_p1  destination-address any
```

```
user@host# set policy-set pset1 policy pset_p1  match application any
user@host# set policy-set pset1 policy pset_p1 then permit
user@host# set default-policy deny-all
```

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.

```
user@host# show security policies
```

```
from-zone dc to-zone cloud-1 {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application junos-vxlan;
        }
        then {
            permit {
                tunnel-inspection {
                    ins-pf1;
                }
            }
        }
    }
}
from-zone cloud-1 to-zone dc {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application junos-vxlan;
        }
        then {
            permit {
                tunnel-inspection {
                    ins-pf1;
                }
```

```
            }
        }
    }
}
policy-set pset1 {
    policy pset_p1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
default-policy {
    deny-all;
}
```

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

Verification

IN THIS SECTION

Verify tunnel inspection profiles and VNI

Purpose

Verify that the tunnel inpection profile and VNI are confugured..

Action

From operational mode, enter the `show security tunnel-inspection profiles ins-pf1` and `show security tunnel-inspection vnis` commands.

```
user@host> show security tunnel-inspection profiles ins-pf1
node0:
--------------------------------------------------------------------------
Logical system: root-logical-system
  Profile count: 1
  Profile: ins-pf1
    Type: VXLAN
    Vxlan count: 1
    Vxlan name: vx1
    VNI count: 4
      VNI:r1, r2, r3, r4
      Policy set: pset1
      Inspection level: 1
```

```
user@host> show security tunnel-inspection vnis
node0:
--------------------------------------------------------------------------
Logical system: root-logical-system
  VNI count: 5
  VNI name: r1
      VNI id count: 1
      [160 - 200]
  VNI name: r2
      VNI id count: 1
      [155 - 155]
  VNI name: r3
      VNI id count: 1
      [300 - 399]
  VNI name: r4
      VNI id count: 1
      [100 - 120]
  VNI name: v1
      VNI id count: 1
      [1 - 100]
```

Meaning

The output displays that the VXLAN feature is enabled and there are no safe search redirects and safe search rewrites.

Verify Safe Search Function

Purpose

Verify that the safe search feature is enabled for Content Security Web filtering solutions.

Action

From operational mode, enter the `Show security flow tunnel-inspection statistic` command to view the tunnel-inspection statistics.

```
user@host> show security flow tunnel-inspection statistics
node0:
--------------------------------------------------------------------------


  Flow Tunnel-inspection statistics:
  Tunnel-inspection statistics of FPC4 PIC1:
  Tunnel-inspection type VXLAN:
    overlay session active:            0
    overlay session create:          269
    overlay session close:           269
    underlay session active:           0
    underlay session create:         566
    underlay session close:          566
    input packets:       349717
    input bytes:      363418345
    output packets:      348701
    output bytes:     363226339
    bypass packets:         501
    bypass bytes:         50890

  Tunnel-inspection statistics of FPC4 PIC2:
  Tunnel-inspection type VXLAN:
    overlay session active:            0
    overlay session create:          270
    overlay session close:           270
    underlay session active:           0
```

```
    underlay session create:          586
    underlay session close:           586
    input packets:       194151
    input bytes:      200171306
    output packets:      193221
    output bytes:     199987258
    bypass packets:         617
    bypass bytes:         92902

  Tunnel-inspection statistics of FPC4 PIC3:
  Tunnel-inspection type VXLAN:
    overlay session active:             0
    overlay session create:           275
    overlay session close:            275
    underlay session active:            0
    underlay session create:          615
    underlay session close:           615
    input packets:       216486
    input bytes:      222875066
    output packets:      213827
    output bytes:     222460378
    bypass packets:        2038
    bypass bytes:        270480

  Tunnel-inspection statistics summary:
  Tunnel-inspection type VXLAN:
    overlay session active:             0
    overlay session create:           814
    overlay session close:            814
    underlay session active:            0
    underlay session create:         1767
    underlay session close:          1767
    input packets:       760354
    input bytes:      786464717
    output packets:      755749
    output bytes:     785673975
    bypass packets:        3156
    bypass bytes:        414272

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


  Flow Tunnel-inspection statistics:
```

```
Tunnel-inspection statistics of FPC4 PIC1:
Tunnel-inspection type VXLAN:
  overlay session active:           0
  overlay session create:         269
  overlay session close:          269
  underlay session active:          0
  underlay session create:        566
  underlay session close:         566
  input packets:          0
  input bytes:            0
  output packets:         0
  output bytes:           0
  bypass packets:         0
  bypass bytes:           0

Tunnel-inspection statistics of FPC4 PIC2:
Tunnel-inspection type VXLAN:
  overlay session active:           0
  overlay session create:         270
  overlay session close:          270
  underlay session active:          0
  underlay session create:        586
  underlay session close:         586
  input packets:          0
  input bytes:            0
  output packets:         0
  output bytes:           0
  bypass packets:         0
  bypass bytes:           0

Tunnel-inspection statistics of FPC4 PIC3:
Tunnel-inspection type VXLAN:
  overlay session active:           0
  overlay session create:         275
  overlay session close:          275
  underlay session active:          0
  underlay session create:        615
  underlay session close:         615
  input packets:          0
  input bytes:            0
  output packets:         0
  output bytes:           0
  bypass packets:         0
```

```
    bypass bytes:             0

  Tunnel-inspection statistics summary:
  Tunnel-inspection type VXLAN:
    overlay session active:             0
    overlay session create:           814
    overlay session close:            814
    underlay session active:            0
    underlay session create:         1767
    underlay session close:          1767
    input packets:            0
    input bytes:              0
    output packets:           0
    output bytes:             0
    bypass packets:           0
    bypass bytes:             0
```

Meaning

The output displays that the VXLAN feature is enabled and there are no safe search redirects and safe search rewrites.

SEE ALSO

tunnel-inspection

Group-Based Policies in VXLAN Environments

IN THIS SECTION

Overview

IN THIS SECTION

Integrating Group-Based Policy (GBP) with Virtual Extensible LAN (VXLAN) architecture facilitates advanced microsegmentation within your networking environment. This functionality empowers you to enforce tag-based policies where policies are driven by business-centric tags rather than traditional network topology constraints.

By configuring source tag and destination tag match options, you gain granular control over network access, allowing for sophisticated traffic management. The system leverages reserved fields in the VXLAN header to apply policies across network segments, ensuring flexible traffic isolation and enhanced access control through Endpoint Groups (EPGs). You can manage group tags using various identifiers like MAC addresses, VLANs, RADIUS server assignments, or controllers, offering adaptable tag management.

SRX Series support tag-based match conditions in security policies to enforce micro-segmentation.

Juniper switches have supported the group-based policy model ((EVPN-VXLAN Group-Based Policies) and micro-segmentations, and now the SRX Series Firewall extend this functionality by incorporating GBP into its security policies. We recommend you to read Micro and Macro Segmentation using Group Based Policy in a VXLAN before you proceed with this topic.

For the complete list of supported features and platforms, see EVPN-VXLAN group-based policies in Feature Explorer.

Key Features

- Endpoint Grouping: Devices and users are categorized into logical groups based on their roles, functions, or security requirements, regardless of their physical location in the VXLAN fabric.

- Policy Definition: Security policies are defined between these groups, specifying allowed interactions, which are then enforced across the VXLAN overlay.
- Consistent Policy Application: Policies are consistently applied regardless of the physical location of devices within the network, a key benefit in VXLAN's location-independent architecture.
- Scalability: As new devices are added to a group, they automatically inherit the group's security policies, aligning well with VXLAN's ability to scale across large data center networks

Benefits of Integrating GBP with VXLAN

- Improve operational efficiency by simplifying the configuration process by allowing you to implement consistent security policies across enterprise network domains.
- Enhance network security by allowing granular control over access based on business-centric tags, reducing the risk associated with unauthorized access.
- Facilitate efficient traffic management by enabling microsegmentation, which isolates network segments and controls interactions between distinct EPGs.
- Support dynamic policy adjustments, making it easier to adapt to changing business requirements without needing to redesign network topology.
- Provide flexibility in tag management through various identifiers, allowing seamless integration with existing infrastructure and simplifying the implementation of policies.

Introduction

In the context of EVPN VXLAN, especially when implementing microsegmentation, the following terms are fundamental to understanding how traffic is classified, controlled, and segmented across the network.

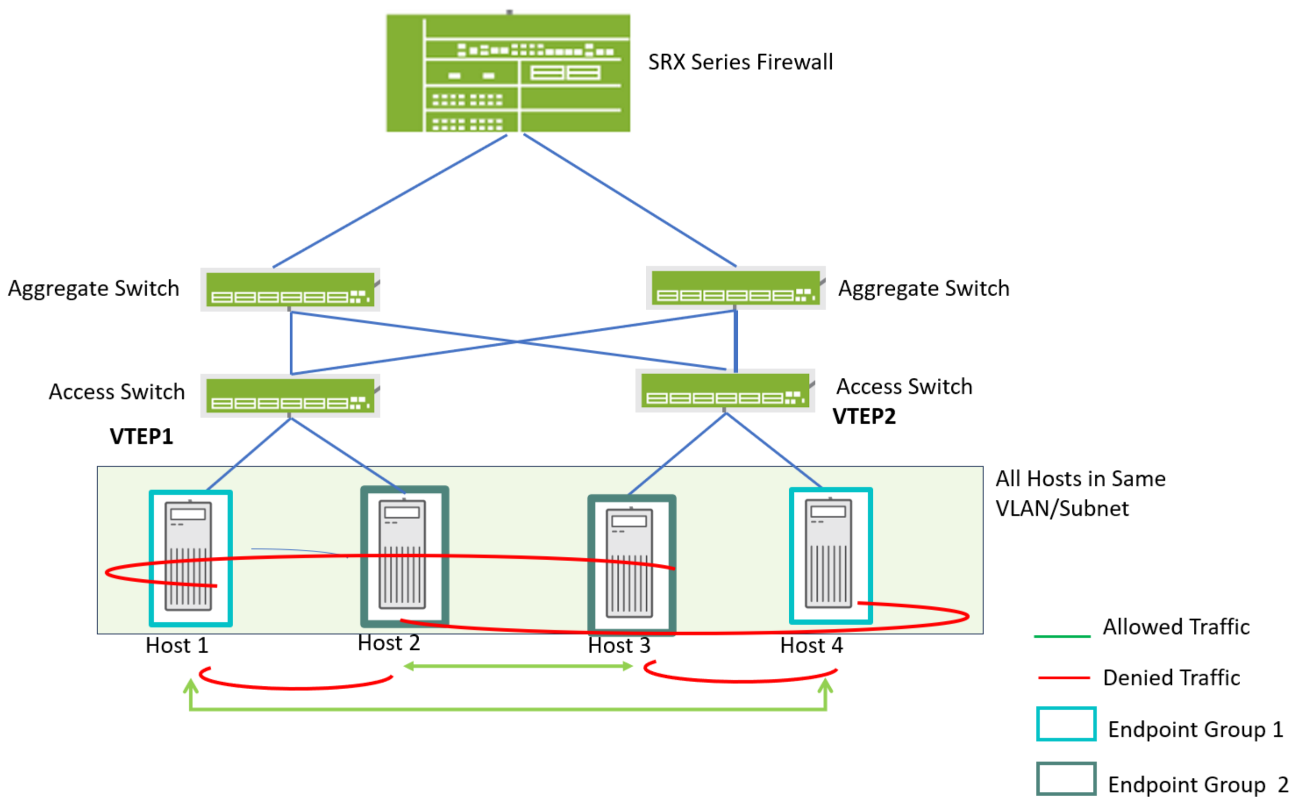
- **Endpoint Group (EPG)** is a logical grouping of endpoints (like VMs, containers, or bare-metal hosts) that share common policy requirements. These groups are used to define which endpoints can communicate with each other. based on attributes like IP subnet, VLAN, VXLAN VNID, or tags. These groups are used to apply consistent security policies across dynamic workloads.
- **Group-Based Policy (GBP)** is a policy model that defines how traffic flows between different EPGs. These policies can control communication between endpoint groups based on identity, not just IP or port.
- **Scalable Group Tags (SGTs)** are 16-bit metadata identifiers assigned to endpoints—such as virtual machines, containers, or hosts—to indicate their group membership. The term GBP tag is a broader reference to the use of these identifiers for enforcing group-based policies across the network. In this document, we use the term **GBP tags** to refer to these identifiers

What is Microsegmentation with GBP?

Microsegmentation allocates users, servers, VMs, and devices to endpoint groups and defines group-based policies between endpoint groups to manage traffic control between endpoints.

Following image shows a portion of VXLAN topology.

Figure 11: Microsegmentation Using Endpoint Groups



In this illustration, SRX Firewall at the spine layer acts as centralized security and policy enforcement. Four Hosts (Host1, Host2, Host3, Host4) connected to the access switches. These four hosts belongs to the same VLAN/subnet. For example, assume that the requirements are as follows:

- Host1 and Host4 can communicate,
- Host2 and Host3 can communicate.
- Host1 and Host4 must not communicate with Host2 and Host3.

To address this requirement, hosts grouped into endpoint groups (EPG1 and EPG2) as follows:

- Host1 (on Switch1) and Host4 (on Switch2) are added to endpoint group 1(EPG1).

- Host2 (on Switch 1) and Host3 (on Switch2) are added to endpoint group 2(EPG2).

Once the endpoints are grouped, intra group access and isolation or inter group access or isolation can be defined. That is, both the access switches are configured with a policy that if source group is EPG1 and destination group is EPG2, deny the traffic and vice-a-versa. Similarly, another set of policies are created that if source group and destination group are same, allow the traffic. As a result:

- Communication between Host2 and Host3 is allowed as both are part of EPG2.
- Communication between Host1 and Host4 is allowed as both are part of EPG1.
- Communication between Host1 and Host2/Host 4 is not allowed as hosts are in different EPGs.
- Communication between Host3 and Host4/Host 2 is not allowed as hosts are in different EPGs..

Group Tag Assignment

GBP uses tags to mark traffic and to enforce policy. The assignment process involves mapping each endpoint to a specific tag based on its business function, which is then utilized in the policy lookup process to enforce the desired communication patterns. In campus networks, tags can be assigned to endpoints in one of the following methods.

- GBP tags—Tags based on various matches on the ingress interface including:
  - MAC address
  - Port
  - VLAN
  - Port, VLAN
  - Subnet/IP Address
- RADIUS server assigned tags—Network environments using RADIUS servers for network access control. Endpoints are placed in VLANs based on the type of endpoint or the user authorization and device fingerprinting. RADIUS server send the group tag in Juniper VSA. The ingress access switch can associate the group tag sent by the RADIUS server to all traffic generated by that MAC address.
- Controller assigned tags—Network environments managed by a controller like Contrail Enterprise Multicloud, tags are assigned to switch ports or endpoints connected to switch ports. Switch can associate the tag to all traffic from these endpoints.

How GBP Tags Work?

- Each endpoint—such as a VM, container, or host—is dynamically assigned a GBP tag based on its role or function (e.g., web server, database server, admin workstation).

- The GBP tag is propagated along with the traffic, either embedded in the VXLAN header or carried as metadata, ensuring that group identity travels with the packet.

- SRX Series Firewalls, or other policy enforcement points inspect the GBP tag to determine how traffic should be handled according to defined group-based policies.

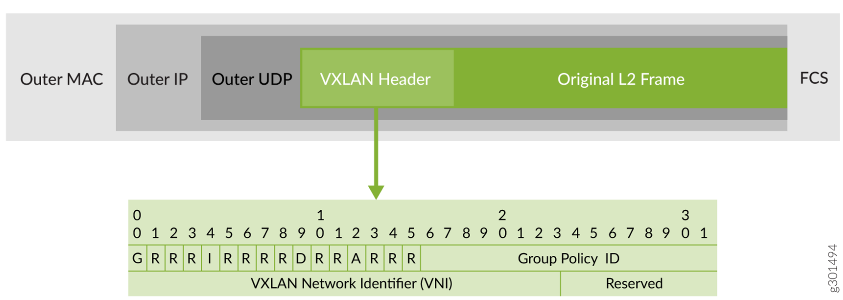
- Security policies are applied by matching source GBP tags and destination GBP tags, allowing enforcement decisions to be made based on group relationships rather than IP addresses or network topology

This approach enables organizations to enforce policies that reflect business logic and organizational structure, rather than being constrained by static network constructs like VLANs or subnets.

VXLAN Header for GBP

VXLAN-GBP leverages reserved fields in the VXLAN header to carry the GBP tags assigned to the frame. Following figure is an example of 16-bit Group Policy ID field .

Figure 12: VXLAN Header for GBP



Enforcement Challenges

When a packet is encapsulated at the source VTEP, it includes the GBP tag of the source endpoint in the VXLAN header. This allows downstream devices to know who sent the traffic. The GBP tag of the destination endpoint is typically not included in the VXLAN header. It's only known at the destination VTEP, which has local knowledge of the endpoint it serves.

If a firewall or policy engine (like SRX) is sitting in the middle of the fabric, it may only see the source tag and not the destination tag, making it hard to apply GBP rules that depend on both. In this case, to enforce policies based on both source and destination GBP tags, the best place is the egress VTEP—the switch that knows the destination endpoint and its group tag. This ensures accurate policy enforcement.

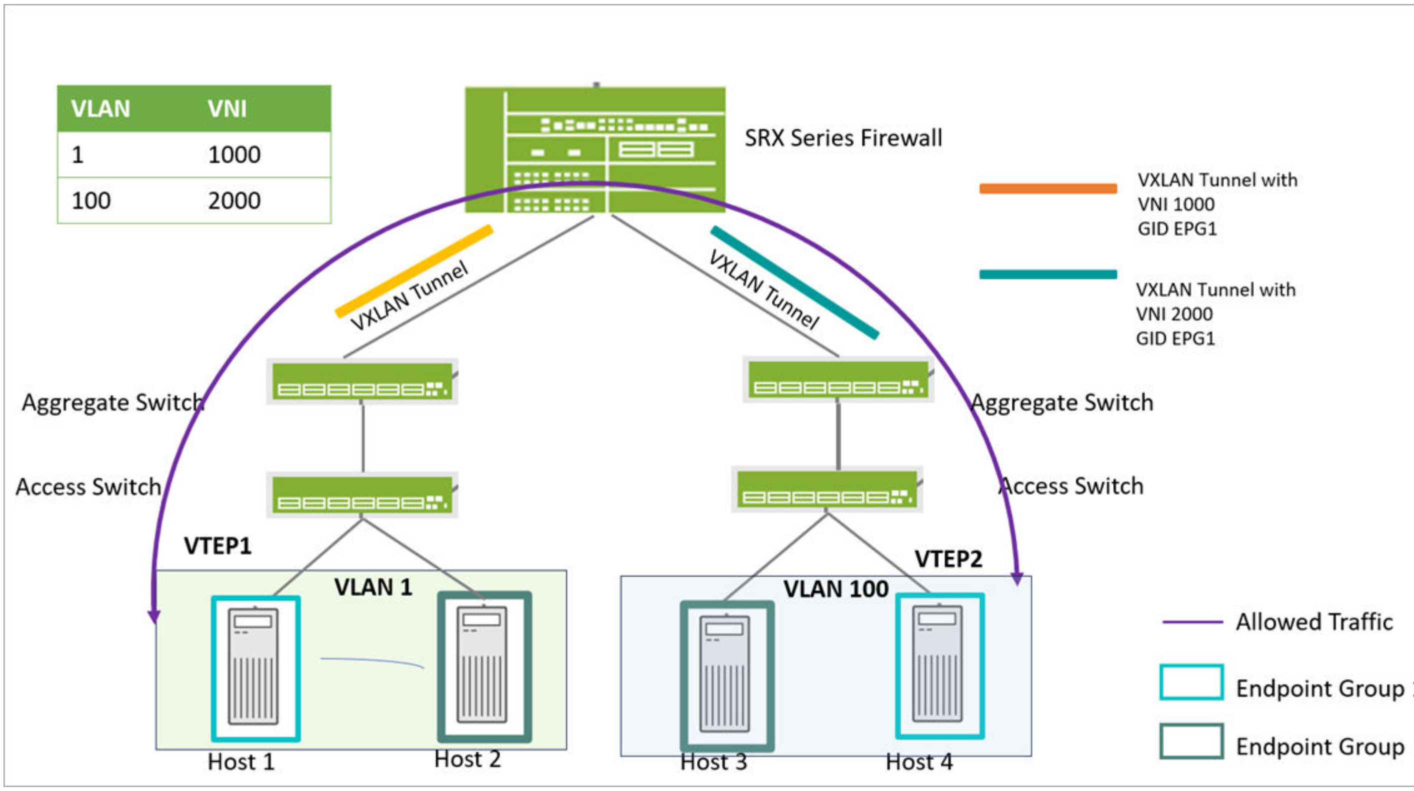
To enable tag-based filtering at ingress or gateway devices, the network must support a mechanism to share group tag information for all endpoints across the fabric. Example: EVPN Type 5 routes (IP Prefix routes) can carry BGP communities that include GBP tags metadata. This setting allows every device in the overlay (including SRX firewalls) to learn the GBP tags of all endpoints, not just the ones locally connected.

Group Tag Transfer in Inter-VXLAN Networks

In a VXLAN (Virtual Extensible LAN) environment, traffic flow between different VXLANs (often referred to as VNIs or Virtual Network Identifiers) requires special handling because VXLAN is designed to extend Layer 2 networks across Layer 3 infrastructure. In such cases, the source group ID must be preserved across VXLAN tunnels to ensure that any policies or security measures associated with the group are maintained throughout the traffic flow.

Following illustration shows the process involved in routing traffic between different VXLAN segments (VNIs) using a Layer 3 gateway that can handle VXLAN encapsulated traffic.

Figure 13: Group Tag Transfer in Inter-VXLAN Networks



Scenario overview:

- Need to establish communication between Host1 and Host4.

- Host1 is located in a VXLAN identified by VNI 1000.
- Host4 is located in a different VXLAN identified by VNI 2000.
- Host1 and Host4 are part of same endpoint group (EPG2).

Traffic flow and inter-VXLAN routing for source group tag preservation:

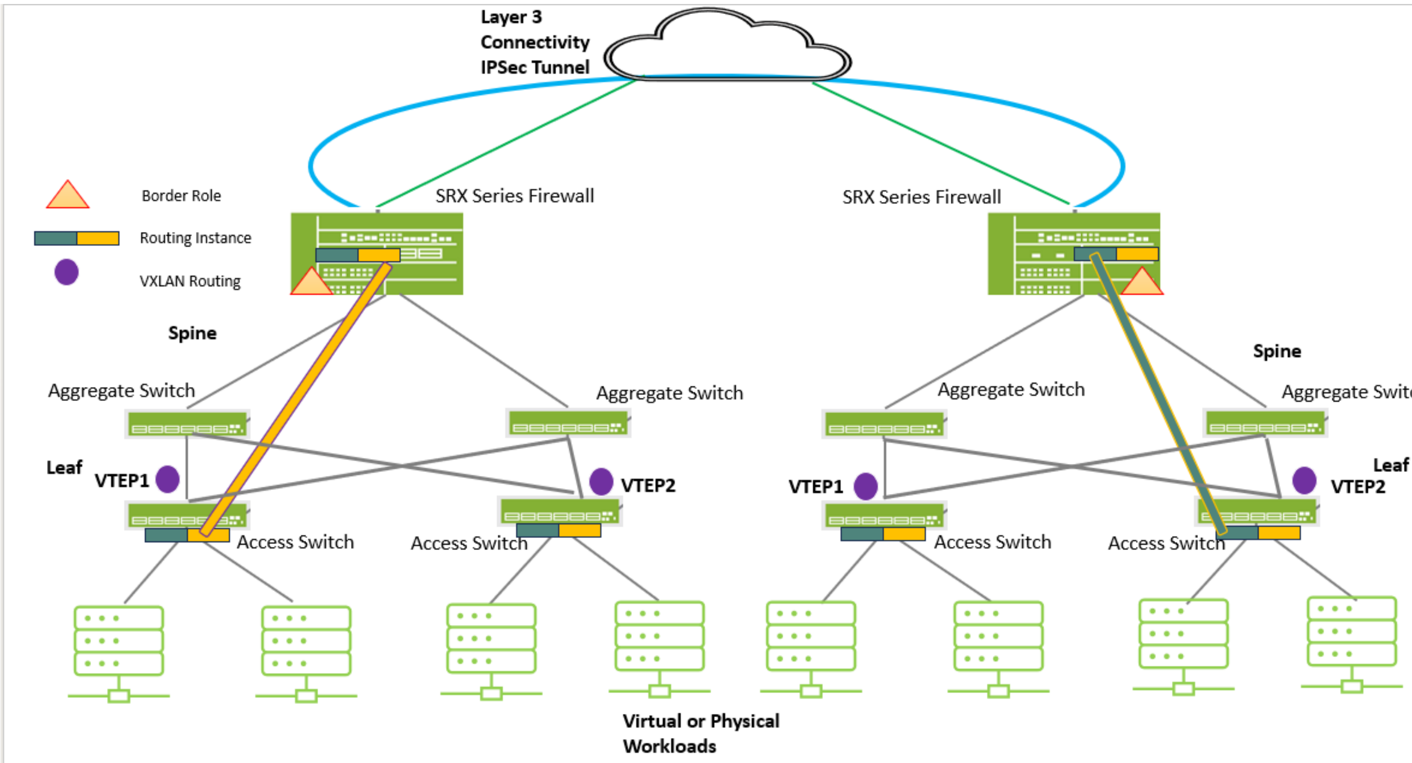
1. Host1 sends a packet destined for Host4. VTEP1 (VXLAN Tunnel Endpoint 1), which is associated with Host1's VNI (1000), receives this packet. Since Host4 is in a different VXLAN (VNI 2000), VTEP1 forwards the packet to the default gateway for VNI 1000, which is L3 Gateway (SRX Series Firewall in this example). Here, the SRX Series Firewall can act as VTEP device to perform encapsulation and de-encapsulation.
2. VTEP1 encapsulates the packet with VXLAN headers, including the EPG1 (Endpoint Group) group ID, which is a metadata identifier used for policy enforcement. The encapsulated packet is sent to the Layer 3 Gateway.
3. The Layer 3 gateway receives the VXLAN-encapsulated packet. It decapsulates the packet to examine the inner payload and source group ID. The gateway is responsible for routing the packet between different VNIs, in this case, from VNI 1000 to VNI 2000.
4. Layer 3 gateway re-encapsulates the packet with VXLAN headers for forwarding to VTEP2 (associated with Host4's VNI, 2000). It ensures that the original source group ID (EPG1) is preserved in the VXLAN header during this re-encapsulation process.
5. VTEP2 receives the encapsulated packet from Layer 3 Gateway. It decapsulates the packet and delivers it to Host4 in VNI 2000.

To effectively manage inter-VXLAN traffic with group tag preservation, you must configure gateway routers to handle encapsulation and decapsulation processes across VXLAN tunnel endpoints (VTEPs). This configuration is required to preserve source group tags during transit, allowing consistent policy enforcement across different network segments.

Inter-Site or External Communication

Following image shows spine-and-leaf EVPN-VXLAN topology for comminication between two datacenters.

Figure 14: Inter-Site Communication



In this topology, SRX Series Firewall acts as a Layer 3 gateway for traffic between VXLAN segments (that is, between different subnets or VNIs). It establishes IPsec tunnels for inter-DC traffic ensuring encrypted communication between sites or external networks.

When host traffic traverses the spine-leaf topology, the system first encapsulates the packet with VXLAN headers. Then, it determines if additional encapsulation (like IPSec) is needed. If so, the SRX prepares the packet for the next tunnel stage, ensuring secure and policy-compliant delivery.

For additional information on GBPs, see Micro and Macro Segmentation using Group Based Policy in a VXLAN. For configuration on SRX Series Firewalls in EVPN-VXLAN, see Tunnel Inspection for EVPN-VXLAN by SRX Series Devices.

Configuration of Group Based Policies

To effectively implement VXLAN group-based policy, understand the process of configuration sequence and options. This section provides configuration sequence and samples related to group-based policies in EVPN-VXLAN deployments. Ensure that the EVPN-VXLAN baseline, including both underlay and overlay configurations, is properly set up and operational.

Configuration Sequences

To implement GBP effectively, you must:

1. **Define GBP tags:**

   Assign GBP tags, which are numeric identifiers, to endpoints to classify them into logical security groups. These tags help enforce identity-based policies across the network.

   - Static Assignment: Configure GBP tags directly on switch ports.
   - Dynamic Assignment: Use RADIUS and 802.1X authentication on switches to assign GBP tags based on user/device identity during login. See Assigning SGTs Using 802.1X in Micro and Macro Segmentation using Group Based Policy in a VXLAN.

   The maximum number of GBP tags that can be configured for both source and destination is 128.

2. **Create GBP Tag Assignment Filters:** Set up filters on switches to assign GBP tags to incoming traffic. These filters can be based on Interface (port), MAC address, or user authentication results (e.g., RADIUS attributes). This ensures that traffic entering the VXLAN fabric is correctly tagged with its group identity for policy enforcement downstream.

3. **Configure GBP Policy Enforcement Filters:** Develop policies that enforce security measures on traffic based on the assigned GBP tags, controlling which traffic is permitted or blocked to achieve segmentation.

4. **Enable VXLAN-GBP Encapsulation:** Configure VXLAN to incorporate the GBP tag within the VXLAN header's Group Policy ID field, facilitating tag propagation across the VXLAN fabric.

5. **Apply GBP Policies at Enforcement Points:** By default, enforcement occurs at the egress switch where both source and destination GBP tags are available. Juniper also supports optional ingress enforcement, requiring destination tag propagation to the ingress point.

6. **Verify and Monitor:** Utilize operational commands to ensure GBP tag assignment, policy enforcement, and VXLAN encapsulation are functioning correctly, confirming that policies are applied as intended.

Configuration Samples

GBP configuration differs depending on whether you're running on a Centrally Routed and Bridging (CRB) overlay or an Edge Routed and Bridging overlay. For details, see Micro and Macro Segmentation using Group Based Policy in a VXLAN.

On Access or Aggregate Switch

1. Configure a firewall filter named "TEST-1" with micro-segmentation capabilities. Specify a condition for term "t1" within the filter. It matches IPv4 traffic and IPv6 traffic originating from the subnet

20.20.20.0/24 and 2000::/64 respectively. Next define the action for traffic that matches the conditions specified in term "t1". In this case, a "gbp-tag" (group-based policy tag) with a value of 200 is applied to the matched traffic.

```
[edit]
user@host# set firewall family any filter TEST-1 micro-segmentation
user@host# set firewall family any filter TEST-1 term t1 from ip-version ipv4 address
20.20.20.0/24
user@host# set firewall family any filter TEST-1 term t1 from ip-version ipv6 address
2000::/64
user@host# set firewall family any filter TEST-1 term t1 then gbp-tag 200
```

2. Configure GBP policy enforcement. Packets with GBP source tag 100 and GBP destination tag 200 will match on term t100-200 and be accepted. Packets with GBP source tag 100 and GBP destination tag 300 will match on term t100-300 and be discarded.

```
[edit]
user@host# set firewall family any filter gbp-policy term t100-200 from gbp-src-tag 100
user@host# set firewall family any filter gbp-policy term t100-200 from gbp-dst-tag 200
user@host# set firewall family any filter gbp-policy term t100-200 then accept
user@host# set firewall family any filter gbp-policy term t100-300 from gbp-src-tag 100
user@host# set firewall family any filter gbp-policy term t100-300 from gbp-dst-tag 300
user@host# set firewall family any filter gbp-policy term t100-300 then discard
```

3. Enable the following statement to perform the policy enforcement at the ingress node.

```
[edit]
user@host# set forwarding-options evpn-vxlan gbp ingress-enforcement
```

Ingress enforcement saves network bandwidth by discarding tagged packets at the ingress that would otherwise be discarded at the egress. To support policy enforcement at or closer to the ingress, we propagate the MAC and IP-MAC based tags across the network using extended BGP communities within EVPN Type 2 and Type 5 routes. For more details, see *Policy Enforcement at the Ingress and Tag Propagation* section in Micro and Macro Segmentation using Group Based Policy in a VXLAN.

4. Associate the GBP filter to a routing instance. Within the routing instance, configure the EVPN-VXLAN GBP ingress source tag to use the `TEST-1` filter.

```
[edit]
user@host# set routing-instances R1 forwarding-options evpn-vxlan gbp ingress-src-tag filter
TEST-1
```

5. On interface `ge-0/0/1`, unit 0, the filter chain `TEST-1` is applied, which ensures that the source GBP tag is pushed into the packet header.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 filter chain TEST-1
```

On SRX Series Firewall

1. A security policy `zone-pol1` is established from the `trust` zone to the `untrust` zone.

   The policy matches traffic with the many criteria including Source GBP tag: `200`. If the traffic matches all these criteria, the policy permits the flow:

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match
source-address any
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match
destination-address any
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match
application any
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match
dynamic-application any
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match gbp-
src-tag 200
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1 match gbp-
dst-tag 400
user@host# set security policies from-zone trust to-zone untrust policy zone-pol1then permit
```

2. Verify policy details on the firewall:

```
usr@hhost# show security policies
Default policy: permit-all
```

```
Default policy log Profile ID: 0
Pre ID default policy: permit-all
Default HTTP Mux policy: permit-all
From zone: trust, To zone: untrust
  Policy: zone-pol1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1, Log
Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: any
    Source identity feeds: any
    Destination identity feeds: any
    Gbp source tags: 200
    Gbp destination tag: 400
    Action: permit, log
```

SEE ALSO

Security Policies for VXLAN | 234

6

CHAPTER

Security Policies for Web Proxy

IN THIS CHAPTER

Explicit Web Proxy

IN THIS SECTION

Explicit Web Proxy

IN THIS SECTION

Explicit Proxy provides a method for steering traffic from any client device to the SRX Series Firewall. The SRX Series Firewall accepts connections from clients, resolves DNS, forwards connections to the specified destination servers, and then gets the response from the server on behalf of the client. In such configuration, the firewall acts an intermediary between clients and servers. Here, all communication between client and server goes through the firewall that is configured as proxy server.

You can configure your SRX Series Firewall interface as explicit web proxy for applying proxy for IPv4 HTTP and HTTPS traffic. Explicit web proxy support is not available for IPv6 traffic.

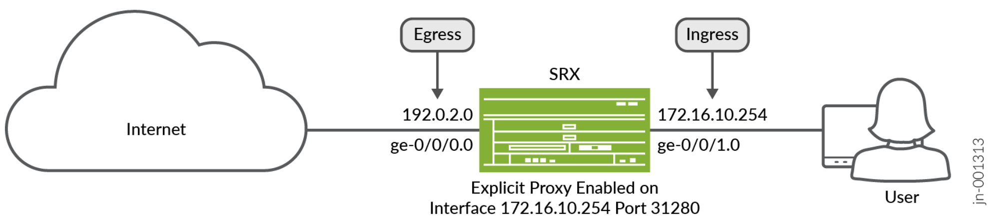
To deploy explicit proxy, manually configure the browser's settings on client device to send requests to SRX SeriesFirewall. In most standard browsers, you can specify the proxy address and port.

SRX Series Firewalls support explicit proxy configuration to obtain the user or device identity information from active directory, identity-management server, LDAP server, and physical SRX Series Firewalls.

How Explicit Proxy Works?

In this example, a client initiates HTTP connection to reach www.example.com. Client device first connects with SRX Series Firewall acting as explicit proxy on (172.16.10.254 and port 31280).

Figure 15: Explicit Web Proxy



The client network connects to the SRX Series Firewall on ge-0/0/1 interface with IP address 172.16.10.254. SRX Series Firewall connects to Internet using the interface ge-0/0/0 with IP address 192.0.2.0.

Prerequisite

- Ensure that the client configure proxy settings on the client browser.

For each session initiated by the client browser, the SRX Series Firewall creates two sessions:

S1: Session originating from client browser to explicit web proxy

S2: Session originating from explicit web proxy to actual destination server.

Table 27 on page 260 provides details on the explicit web proxy sessions.

Table 27: Explicit Proxy Session Details

Session Type	Source IP/Port	Destination IP/Port	Policy	Comments
Client to SRX Series Firewall (S1)	Client IP / dynamic port range	SRX Series Firewall interface IP (172.16.10.254) / fixed port (31280)	Security policy/ unified policy (explicitly configured on SRX Series Firewall)	Client traffic directly comes to the SRX Series Firewall interface where explicit proxy profile is configured.

Table 27: Explicit Proxy Session Details *(Continued)*

Session Type	Source IP/Port	Destination IP/Port	Policy	Comments
SRX Series Firewall to actual destination server (S2)	SRX Series Firewallegress interface IP (192.0.2.0)/ dynamic port range	End server as resolved by DNS or in explicit proxy request	Implicitly inherited from S1	SRX Series Firewall establishes the connection with actual server.

Benefits

- Explicit web proxy secures network by controlling and filtering the inbound and outbound traffic.
- Explicit web proxy performs DNS resolution on client's behalf.

Steps to Configure Explicit Proxy on SRX Series Firewall

To manage explicit proxy for connections to your network, you must:

1. Configure the explicit proxy profile.
2. Configure explicit proxy on an interface. This interface must be connected to client network. The client browsers use this IP address to forward requests to the SRX Series device. You can configure and attach multiple explicit proxy profiles to a particular IP address in the interface. However, you must ensure that there must not be overlapping ports between the explicit proxy profiles.
3. Use security policies to control the explicit web proxy traffic.
4. Configure default-policy for the explicit proxy.

Configure Explicit Proxy

1. Configure explicit web proxy profile `exp-proxy-profile` to reach the interface `ge-0/0/0`.

```
user@host# set services web-proxy explicit-proxy profile exp-proxy-profile listening-port
31280
user@host# set services web-proxy explicit-proxy profile exp-proxy-profile preferred-egress-
source-ip default-egress-ip
```

The `default-egress-ip` is the egress source IP address associated with outgoing interface.

2. Configure interface that is used to enable explicit web proxy.

```
user@host# set interfaces ge-0/0/1 unit 0 explicit-proxy profile exp-proxy-profile
```

Configure Security Policy

You must configure and enforce security policies to manage the traffic for the explicit proxy. Explicit proxy profile needs a set of unique security policies or unified policies. The firewall determines which profile to leverage for a policy lookup based on the ingress interface and port combination. Once the firewall identifies the explicit proxy profile for a flow, it performs a policy lookup.

SRX Series Firewall uses the following sequence for the policy lookup:

- Source IP address, source-port, protocol, and source identity
- DNS-based destination IP resolution
- URL category detection
- Dynamic Layer 7 application match
- DNS-based destination resolved IP reputation
- Hardcoded destination IP address or reputation of hardcoded destination IP address

You can configure the explicit proxy profile rule-base using the following statement:

You can notice that this policy, similar to the global policies, does not need security zones.

To attach a security policy with explicit proxy profile, the profile name mentioned in policy configuration must match with the name of the explicit proxy profile configured under web-proxy services (`set services web-proxy explicit-proxy profile <profile-name>`).

- Define a security policy to control the explicit web proxy traffic.

```
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match
source-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match
destination-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match
application any
```

```
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match
dynamic-application any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy then
log session-close
commit
```

Default Policy for Explicit Proxy

In case the traffic matches to any of the explicit proxy profiles but does not match any of the policies under the explicit proxy profile, the firewall applies the default policy action. You can configure the default policy in the explicit proxy profile.

In case no matching explicit proxy profile found for a given traffic, the firewall performs the policy lookup based on configured zone and global policies.

You can configure only one default policy per explicit proxy profile.

Limitations

For explicit proxy profile policies, the match condition does not support:

- Source or destination zone
- Source and destination Layer 3 VPN VRF group

Post-match application services do not support:

- Secure web proxy
- GPRS Tunneling protocol
- GPRS stream control transport protocol (SCTP)
- Unified Access control enforcement of policy (UAC)
- WAN acceleration (Legacy WX)
- Legacy Intrusion detection and prevention.
- APBR

SEE ALSO

Configuring Security Policies | 96

Use Case Scenarios

IN THIS SECTION

Configure SSL Proxy

Secure Sockets Layer (SSL) Proxy provides deep packet inspection and decryption of outbound SSL or Transport Layer Security (TLS) traffic for security inspection and policy enforcement on Web traffic received.

Ensure to enable SSL proxy to decrypt sessions so that the advanced security services are applied for inspection, detection, and mitigation. For details, see SSL Proxy Configuration Overview.

- Apply the SSL proxy profile, `SSL_FP` to the explicit web proxy profile, `exp-proxy-profile` to permit the traffic.

```
set services web-proxy explicit-proxy profile exp-proxy-profile ssl-proxy profile-name SSL_FP
Commit
```

Configure Content Security Filtering

Content Security provides comprehensive security solution that integrates multiple features like antivirus, anti-spam, content filtering, and web filtering on the received web traffic.

You can apply advanced security service profiles for the features IDP, ATP, AppQos, and so on to the proxy traffic. For details, see Content Security.

- Specify the Content Security policy to be applied on the traffic that matches the conditions specified in the security policy.

```
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
source-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
destination-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
application any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
dynamic-application any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy then 
permit application-services utm-policy CON-SEC-POL
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy then 
log session-close
commit
```

Configure Identity Aware Firewall

Identity Aware Firewall enforces network access policies based on individual user identities, allow or block traffic according to predefined rules associated with each user on the received web traffic.

You can use identity sources such as Active Directory, JIMS, UAC, Aruba Clearpass and so on to authenticate users. For more information on identity source, see Identity-Sources.

- Configure a security policy to use identify parameters that match with the `source-identity` specification.

```
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
source-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
destination-address any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
application any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
source-identity any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy match 
dynamix-application any
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy then 
permit application-services utm-policy ORG_EWF_POL
```

```
set security policies explicit-proxy profile exp-proxy-profile policy exp-proxy-policy then
log session-close
commit
```

NOTE: All the use case features are enabled independently with multiple policies or can be combined on the same policy to expand the threat inspection capabilities.

Transparent Web Proxy

SUMMARY

Learn how to configure a transparent web proxy on SRX Series Firewalls with this step-by-step example.

IN THIS SECTION

You can use Transparent Web proxy to send traffic to an external proxy server and bypass the proxy server for the selected application traffic. Bypassed application traffic will be sent directly to the target webserver.

In addition, the transparent web-proxy functionality supports HTTP/2, allowing you to relay HTTPS traffic without decryption, ensuring secure and efficient data transmission.

Transparent web proxy allows you to route traffic through an external proxy server without the client browser being aware of it. That is, the proxy operates invisibly to the user, requiring no additional authentication or configuration on their part.

When using a transparent proxy, you can specify certain application traffic to bypass the proxy server. For example, if you want traffic from a specific application (like Yahoo) to go directly to the webserver, you can configure the proxy to exempt this traffic. This bypassed traffic will be sent straight to the target webserver, avoiding the proxy server entirely.

As a result, your firewall performs transparent proxy between the client and the webserver for the specified applications and provides better QoS for the application traffic.

Benefits of Transparent Web Proxy

- Enhances the quality of service for specific application traffic by establishing direct connections to the web server.
- Implements distinct security policies for various types of traffic, allowing you to bypass the proxy for trusted applications while directing other traffic through the proxy for further inspection.
- Bypasses the proxy for high-bandwidth applications like video streaming services, reducing the load on the proxy server and improving overall network performance.
- The proxy transparently processes HTTPS traffic via HTTP CONNECT, while seamlessly relaying all other traffic types—like plain HTTP and HTTP/2—to the client's designated external proxy, ensuring broad protocol support without disrupting routing.

Limitations

- SRX Series Firewall does not support transparent web proxy or transparent web proxy feature may not function properly in the following cases:
  - When operating in chassis cluster mode or in Multinode High Availability.
  - When configured with all layer 7 security features except Advanced policy-based routing (APBR).
  - When configured with unified policies (security policies with dynamic applications).
  - When operating in transparent-bridge mode.
  - When the client device and its proxy server are deployed in the same network segment.
  - Transparent proxy bypasses both plain HTTP/2 traffic and HTTP CONNECT requests sent in HTTP/2 frame format.
  - SSL proxying must not be applied to sessions processed through the transparent proxy.

Transparent Web Proxy Overview

IN THIS SECTION

How Transparent Web Proxy Works?

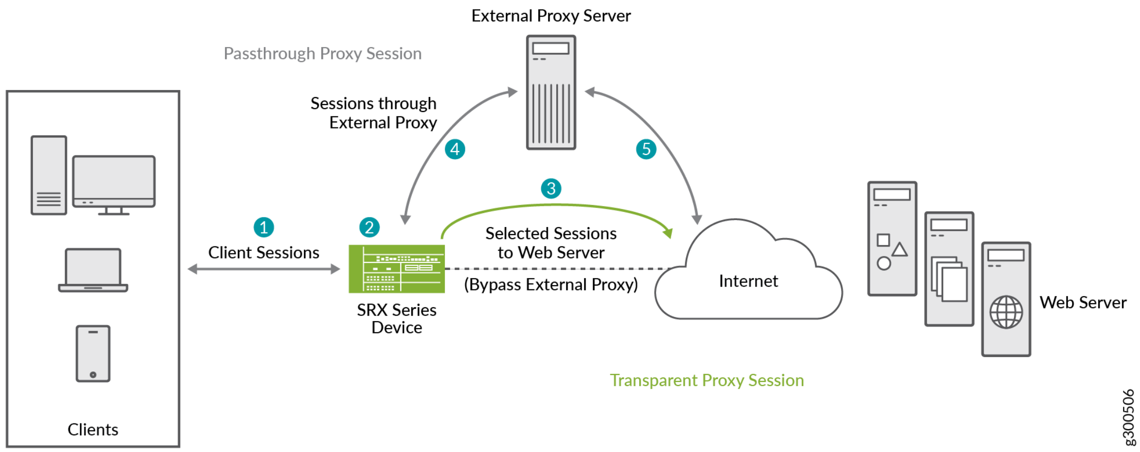
IN THIS SECTION

When the SRX Series Firewall receives a request from a client, it examines the HTTP header to identify the application. Based on the transparent proxy profile, the firewall determines which traffic can bypass the external proxy server. It applies the profile to traffic that matches the security policy rules. Permitted application traffic that matches the dynamic application specified in the profile is directed to the webserver. Otherwise, the permitted traffic is redirected to the configured external proxy server.

For example, if you want to bypass MS Office or Yahoo traffic from external proxy server, you can specify these applications in the transparent web proxy profile. The SRX Series Firewall forwards Yahoo or SMS Office application traffic directly to the server, bypassing the external proxy server. Connections that do not match the applications are routed to the external proxy server.

Following illustrations show how an SRX Series Firewall provides the transparent Web proxy service.

Figure 16: Transparent Web Proxy on SRX Series Firewall



1. The client's browser sends an HTTP connect request to the external proxy server.
2. The SRX Series Firewall intercepts the TCP connections. The device identifies the application in the HTTP header and does a DNS resolution.
3. If the traffic parameters match the security policy rules and the transparent Web proxy profile specifications, the SRX Series Firewall operates in transparent mode. The device uses the client's IP address in transparent mode to initiate a new connection with the webserver, bypassing the external proxy server.
4. For the remaining traffic, the SRX Series Firewall operates in pass-through mode and allows the HTTP connect request to go to the external proxy server. When a client makes a request, the request is sent to the proxy server first, which then forwards the request to the actual server.
5. The server responds to the proxy, and the proxy then sends the response back to the client through SRX Series Firewall.

The SRX Series Firewall performs secure Web proxy through the following steps:

To use transparent Web proxy on your SRX Series Firewall, you must:

1. Create a transparent web proxy profile with external proxy server details and the dynamic application or application group that you want to bypass the external proxy server.
2. Create a security policy to manage the traffic passing through the device.
3. Attach the secure Web proxy profile to the security policy and apply the profile as an application service for the permitted traffic.

Transparent Web Proxy for HTTP/2 Traffic

The transparent web-proxy's support for HTTP/2 allows you to relay encrypted HTTPS traffic using the HTTP/2 protocol without decrypting it. This capability ensures that the ALPN extension used during TLS negotiations is not interfered with, enabling seamless client/server communication. By adopting HTTP/2, your network benefits from features like multiplexing, header compression, and prioritization. These features improve web communication speed and efficiency, offering a more responsive user experience.

Transparent Web Proxy and Secure Web Proxy

IN THIS SECTION

Starting in Junos OS Release 25.2R1, we've renamed the secure web proxy as transparent web proxy.

Read one of the following topic for configuring using transparent proxy:

- If you are using Junos OS version 25.2R1 and later releases, you must configure Transparent Web proxy for same benefits as secure web proxy. See "Example: Configure Transparent Web Proxy" on page 271.
- If you are using Junos OS version before Junos OS 25.2R1, you can continue to use Secure Web proxy. See *Secure Web Proxy*.

CLI Configuration Statements Changes

If you are planning to upgrade to Junos OS Release 25.2R1 and later releases, note the following points regarding using proxy functionality:

All existing secure web proxy related CLI statements and commands are deprecated. That is—Starting in Junos OS Release 25.2R1 secure web proxy functionality is deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration. As a part of this change, the `[edit services web-proxy secure-proxy]` hierarchy and all the configuration options under this hierarchy are deprecated. That is, the hierarchy for transparent proxy configuration statements has changed from `set services web-proxy secure-proxy` to `set services web-proxy transparent-proxy`.

To migrate, you will need to replace existing command hierarchies with the new ones as shown in the following table.

Table 28: Secure Web Proxy Hierarchy Replacements

Previous Hierarchy (Secure Web Proxy)	New Hierarchy (Transparent Web Proxy)
`set services web-proxy secure-proxy`	`set services web-proxy transparent-proxy`
`set security policies from-zone trust to-zone untrust policy apply_webproxy then permit application-services web-proxy profile-name <trans-proxy-profile-name>`	`set security policies from-zone trust to-zone untrust policy apply_webproxy then permit application-services transparent-proxy profile-name <trans-proxy-profile-name>`

These adjustments ensure that your configurations are up-to-date and ready to take advantage of the new features.

Example: Configure Transparent Web Proxy

IN THIS SECTION

You can use the Transparent wb proxy feature to direct the traffic through an external proxy server or bypass it for specified applications on an SRX Series Firewall. By configuring a transparent Web proxy profile with the external proxy server details and applications to bypass, you ensure traffic is sent directly to the target webserver when applicable. The device inspects HTTP headers and applies the web proxy profile based on security policy rules, redirecting authorized traffic accordingly.

In this example, we'll configure transparent web proxy to direct an application traffic to the webserver bypassing external proxy server.

TIP:

Table 29: Time Estimates

Reading Time	15 minutes
Configuration Time	30 minutes

Example Prerequisites

Table 30 on page 272 lists the hardware and software components that support the configuration.

Table 30: Requirements

Hardware requirements	Supported SRX Series Firewalls and vSRX Virtual Firewalls. We've tested this example using vSRX instance.
Software requirements	Junos OS Release 25.2R1. IP address and port number of the external proxy server. Install and configure Application Identification (AppID). For details, see Predefined Application Signatures for Application Identification. A valid application identification feature license on your SRX Series Firewall. See Managing Junos OS Licenses.

Before You Begin

Know more	Security Policies
Learn more	Explicit Web Proxy

Functional Overview

Table 31 on page 273 provides a quick summary of the configuration components deployed in this example.

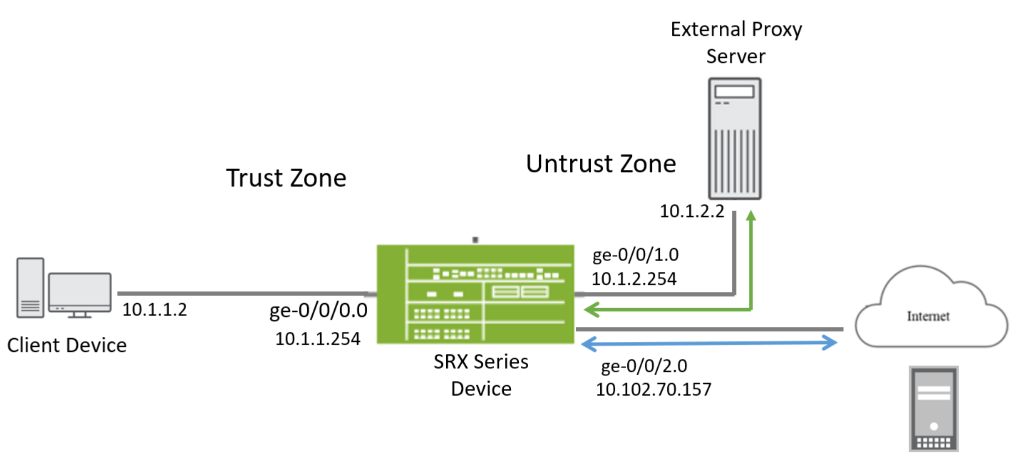
Table 31: Configuration Components

Technologies used	• Transparent web proxy • Security zones and policies
Primary verification tasks	• "Verify Session Details" on page 277 • "Check Transparent Web Proxy Statistics" on page 278

Topology Illustration

Following figure shows the topology used in this configuration example.

Figure 17: Topology For Configuring Transparent Web Proxy



In this example, you configure a transparent web proxy profile on the SRX Series Firewall that forwards most outbound web traffic through the external proxy server. However, traffic destined for specific dynamic applications—such as Yahoo—should bypass the proxy and be forwarded directly to the Internet through the ge-0/0/2.0 interface.

Traffic flow in a transparent web proxy scenario is as follows:

(For regular traffic)

1. The client in the trust zone (IP: `10.1.1.2`) initiates a web request (e.g., to a general website).
2. This traffic reaches the SRX firewall via interface `ge-0/0/0.0`. The firewall evaluates the traffic against the transparent web proxy profile. Since the traffic is not identified as Yahoo , it is redirected to the external proxy server at `10.1.2.2` via interface `ge-0/0/1.0` .
3. The proxy server then forwards the request to the Internet through its own route.
4. The response from the Internet returns to the proxy server, which then sends it back to the SRX via `ge-0/0/1.0`, and the firewall forwards it to the client.

(For Yahoo-specific traffic)

1. The client sends a request to a Yahoo service (e.g., mail.yahoo.com).
2. The SRX firewall receives this on `ge-0/0/0.0` and uses application identification to detect that the traffic is Yahoo-related.
3. Because Yahoo is exempted in the proxy profile, the firewall bypasses the external proxy .
4. Instead, it forwards the traffic directly to the Internet via interface `ge-0/0/2.0` .
5. The response comes back through `ge-0/0/2.0` and is routed directly to the client via `ge-0/0/0.0`.

The firewall enforces zone-based policies to control traffic between Trust and Untrust zones.

NOTE: Our lab environment uses the interface NAT feature to translate internal IPs for outbound Internet access. This example was set up and tested with this lab-specific NAT configuration for outbound traffic from the SRX Series Firewall and does not include NAT configuration details.

Topology Overview

Table 32 on page 274 shows the details of configuration used in this example.

Table 32: Interfaces and IP Address Configuration on Security Devices

Device	Interface	IP Address	Zone	Configured For
SRX Series Firewall	ge-0/0/0	10.1.1.254/24	Trust	Connects to client desktop.
	ge-0/0/1	10.1.2.254/24	Untrust	Connects to proxy server.

Table 32: Interfaces and IP Address Configuration on Security Devices *(Continued)*

Device	Interface	IP Address	Zone	Configured For
	ge-0/0/2	10.102.70.157	Untrust	Connects to Internet.

Configuration Objects:

- Transparent proxy profile:
  - Define the external proxy server's IP (10.1.2.2) and port.
  - Apply the profile to outbound HTTP/HTTPS traffic from the Trust zone.
- Application-based proxy bypass:
  - Use application identification to detect Yahoo traffic.
  - Exempt Yahoo traffic from proxy redirection.
- Traffic flow behavior:
  - **Yahoo traffic**: Routed directly to the Internet via ge-0/0/2.0, bypassing the proxy.
  - **All other web traffic**: Redirected to the external proxy server via ge-0/0/1.0.

Configure Transparent Web Proxy

Use the following steps:

1. Configure interfaces.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.254/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.1.2.254/24
user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.102.70.157/24
```

2. Configure security zones.

```
[edit]
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone untrust host-inbound-traffic system-services all
```

```
user@host# set security zones security-zone untrust interfaces ge-0/0/2.0
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
```

For this specific example, we have set host-inbound-traffic to 'all'. Ensure that you configure host inbound traffic on zones according to your network needs.

3. Enable application identification.

```
[edit]
user@host# set services application-identification
```

4. Create a transparent web proxy profile and provide the IP address and port details of the external proxy server. Additionally, specify the application (Yahoo in this example) whose traffic should be exempt from the proxy server.

```
[edit]
user@host# set services web-proxy transparent-proxy profile yahoo-profile proxy-address
external_proxy ip 10.1.2.2/32
user@host# set services web-proxy transparent-proxy profile yahoo-profile proxy-address
external_proxy port 8080
user@host# set services web-proxy transparent-proxy profile yahoo-profile dynamic-web-
application junos:YAHOO
```

5. Configure security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy policy-for-
transparent-proxy match source-address any
user@host# set security policies from-zone trust to-zone untrust policy policy-for-
transparent-proxy match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy policy-for-
transparent-proxy match application any
user@host# set security policies from-zone trust to-zone untrust policy policy-for-
transparent-proxy then permit application-services transparent-proxy profile-name yahoo-
profile
```

The policy `policy-for-transparent-proxy` applies the transparent web proxy profile `yahoo-profile` for the matching traffic.

Verification

IN THIS SECTION

Use the following show commands to verify the feature in this example.

Table 33: Verification Tasks

Commands	Verification Task
`show services web-proxy transparent-proxy session`	Display transparent web proxy session details.
`show services web-proxy transparent-proxy statistics`	Display transparent web proxy statistics.

Check Transparent Web Proxy Session Detail

Purpose

View and verify the details of transparent web proxy session.

Action

From operational mode, run the following commands:

```
user@host> show services web-proxy transparent-proxy session detail

Transparent Proxy sessions:

Client Session ID : 8590193205, Proxy Session ID: 8590193206
Client: 10.1.2.254/13250 ---> 10.1.2.2/8080
Proxy : 10.1.1.2/35662 ---> 69.147.88.7/443
Proxy Request: CONNECT:www.yahoo.com:443
Dynamic Web App: junos:YAHOO
```

```
Client Session ID : 8590193212, Proxy Session ID: 8590193213
Client: 10.1.2.254/13739 ---> 10.1.2.2/8080
Proxy : 10.1.1.2/35680 ---> 69.147.88.8/443
Proxy Request: CONNECT:www.yahoo.com:443
Dynamic Web App: junos:YAHOO

Client Session ID : 8590193210, Proxy Session ID: 8590193211
Client: 10.1.2.254/24706 ---> 10.1.2.2/8080
Proxy : 10.1.1.2/35672 ---> 74.6.231.20/443
Proxy Request: CONNECT:yahoo.com:443
Dynamic Web App: junos:YAHOO
```

```
 user@host> show services web-proxy transparent-proxy session summary
Transparent Proxy sessions:
Client Session                                  Proxy Session
[8590193288] 10.1.2.254/28677 ---> 10.1.2.2/8080 [8590193289] 10.1.1.2/48870 ---> 69.147.88.7/443
```

Meaning

In these samples, observe the client and proxy session details. The client session extends from the SRX Series Firewall to the proxy server. The proxy session connects the client device directly to the webserver. Additionally, you can observe proxy requests and dynamic web applications.

NOTE: Our lab uses the interface NAT configuration for outbound Internet access. The sample output reflects this setup, showing NATed IPs and ports specific to our lab configuration.

Check Transparent Web Proxy Statistics

Purpose

View transparent web proxy session statistics.

Action

From operational mode, run the following command:

```
user@host> show services web-proxy transparent-proxy statistics
Transparent Proxy :
    Active Transparent proxy sessions          0
    Active Passthrough sessions                0
    Active HTTP passthrough sessions           0
    Active HTTPS passthrough sessions          0
    Total Transparent proxy sessions           4
    Total Passthrough sessions                 0
    Total HTTP Passthrough sessions            0
    Total HTTPS Passthrough sessions           0
```

Meaning

Output displays that the number of transparent web proxy sessions. The proxy has handled four sessions in total, all through the transparent proxy. There are no passthrough (bypassed) sessions have occurred.

Set Commands on All Devices

IN THIS SECTION

Set Commands on SRX Series Firewall

```
set services application-identification
set services web-proxy transparent-proxy profile yahoo-profile proxy-address external_proxy ip
10.1.2.2/32
set services web-proxy transparent-proxy profile yahoo-profile proxy-address external_proxy port
8080
set services web-proxy transparent-proxy profile yahoo-profile dynamic-web-application
junos:YAHOO
```

```
set security policies from-zone trust to-zone untrust policy policy-for-transparent-proxy match
source-address any
set security policies from-zone trust to-zone untrust policy policy-for-transparent-proxy match
destination-address any
set security policies from-zone trust to-zone untrust policy policy-for-transparent-proxy match
application any
set security policies from-zone trust to-zone untrust policy policy-for-transparent-proxy then
permit application-services transparent-proxy profile-name yahoo-profile
set security policies pre-id-default-policy then log session-close
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.254/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.2.254/24
set interfaces ge-0/0/2 unit 0 family inet address 10.102.70.157/24
```

Show Configuration Output

IN THIS SECTION

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

Transparent Web Proxy

```
[edit]
user@host# show services
application-identification;
web-proxy {
```

```
    transparent-proxy {
        profile yahoo-profile {
            proxy-address external_proxy {
                ip 10.1.2.2/32;
                port 8080;
            }
            dynamic-web-application junos:YAHOO;
        }
    }
}
```

Security Policies

```
[edit]
user@host# show security policies
    policy policy-for-transparent-proxy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    transparent-proxy {
                        profile-name yahoo-profile;
                    }
                }
            }
        }
```

Security Zones

```
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
```

```
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/2.0;
        ge-0/0/1.0;
    }
}
```

Interfaces

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.254/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 10.1.2.254/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
```

```
            address 10.102.70.157/24;
        }
    }
}
```

SEE ALSO

transparent-proxy

7

CHAPTER

Security Policies for DNS

IN THIS CHAPTER

DNS Snooping for Security Policies

SUMMARY

Read this topic to understand how DNS snooping feature offers a mechanism for dynamically inspecting and caching DNS responses in real time on security devices.

IN THIS SECTION

Overview

IN THIS SECTION

DNS name servers provide an IP address of the hostname to users. The TTL field in the resource record defines the period for which DNS query results are cached. When the TTL value expires, the name server sends a fresh DNS query and updates the cache.

A policy or NAT source/destination address can be a Fully Qualified Domain Names (FQDN). If the DNS changes, the policy updates with new IP addresses. In some deployments, resolved IP addresses change quickly due to load balancers, which might not provide all IP addresses for a DNS query. Old DNS IP addresses with longer TTL remain valid, but new IP addresses resolve in 4-5 seconds, which might result in unsynchronized FQDN-IP mapping.

To address this issue, SRX Series Firewalls support DNS snooping feature. The DNS snooping feature offers a mechanism for dynamically inspecting and caching DNS responses in real time. When you enable DNS snooping, the system captures DNS response packets as traffic traverse the network, extracting the relevant DNS records and build mapping of FQDN and IP address in a local cache. This cache provides accurate and timely DNS mappings by ensuring that IP addresses associated with Fully Qualified Domain Names (FQDNs) remain current.

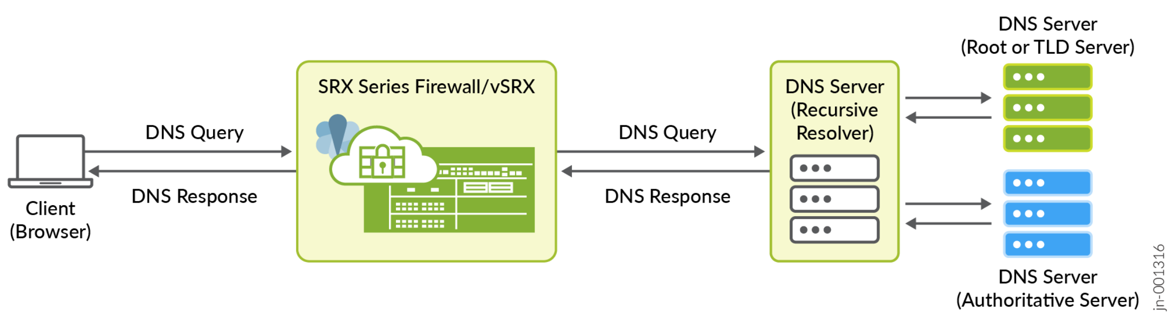
Benefits of DNS Snooping

- Ensures real-time updates of DNS mappings in environments with frequently changing DNS entries.
- Allows for granular control over DNS snooping configuration, enabling you to activate the feature globally or restrict it to specific trusted DNS servers.
- Supports both IPv4 and IPv6 traffic.

How DNS Snooping Works?

DNS traffic originating from the client passes through the SRX Series Firewall. This illustration is a symmetrical traffic case where SRX Series Firewall sees both DNS query and the DNS responses. DNS snooping also supports asymmetrical traffic deployment where the firewall sees only the DNS response.

Figure 18: DNS Snooping on SRX Series Firewall



To resolve a DNS, the client browser sends DNS query to DNS resolver, which in turn resolves the IP using Root server, TLD (top-level domain) server and Authoritative server. Client gets the DNS response. After this exchange, the client starts communication with the server.

As a packet passes through SRX Series Firewall, the firewall uses application identification and deep packet inspection (DPI), to obtain DNS-related contexts. Based on these contexts, the firewall builds a cache of DNS records for FQDNs that are configured in the policy. The cache maintains FQDN, IP, and TTL information. Any updates in the DNS cache, the change propagates to the NAT or security policy module.

NOTE:

- DNS snooping builds DNS cache on SRX Series Firewall for the traffic originated from the end user client and not from one DNS server to another, or host-bound packets, or packets to DNS proxy.
- You can enable either the DNS proxy or DNS snooping at a time.
- We support snooping of DNS traffic over UDP and DNS traffic over TCP (symmetric traffic deployments).

Support for Logical System and Tenant System

DNS snooping configured at the root logical system applies to all logical-systems; any DNS-snooping done at the logical-system level gets included into the system-wide DNS-snooping cache.

DNS Snooping and DNS Module Integration

IN THIS SECTION

DNS Snooping feature also integrates with existing DNS cache module in the RE. This common DNS cache provides comprehensive and up-to-date DNS database.

The system merges entries from following sources to provide data for common DNS cache:

- DNS-resolver that resolves FQDN using explicit DNS-query
- DNS-snooping that resolves FQDN after inspecting the DNS traffic in the dataplane.

The `show security dns-cache` command displays the entries from both DNS-resolver and DNS-snooping.

Security Policies Utilyzing DNS Snooping Cache

In this example, you enable DNS snooping and create a address book with FQDN name. Then create a security policy and add the address book (FQDN name) as destination address. When the traffic matches security policy, the system captures DNS response packets as traffic traverse the network, extracting the relevant DNS records and build mapping of FQDN and IP address in a local cache.

In addition, you can configure a security policy to use the DNS cache and enforce the intended policy. For example, in the following sample, the system obtains data through DNS-snooping, which allows policy P1 to match the desired traffic.

```
[edit]
user@host# set security address-book global address addr1 dns-name www.example.com
user@host# set services dns-snooping global-enable
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-address
addr1
user@host# set security policies from-zone trust to-zone untrust policy P1 match destination-
address any
user@host# set security policies from-zone trust to-zone untrust policy P1 match application any
user@host# set security policies from-zone trust to-zone untrust policy P1 match source-identity
authenticated-user
user@host# set security policies from-zone trust to-zone untrust policy P1 then permit
```

The above configuration ensures that the policy (P1) matches traffic originating from the address associated with "www.example.com". With this configuration, only authenticated users from "www.example.com" will be permitted. This example demonstrates how DNS-snooping-based policies provide precise control and enhance network security by dynamically adjusting to real-time DNS data.

Set DNS Snooping Report Interval

You can control how often DNS-snooping data from the data plane populates in the comon DNS cache using the following statement:

```
[edit]
user@host# set services dns-snooping report-interval  <1..10>
```

You can set the interval between 1 to 10 seconds. The default interval is 5 seconds.

A lower interval propagates data earlier and expedites policy enforcement but increases device communications and frequent policy changes. Use a lower interval when DNS-snooping churn is minimal, as indicated by show services dns-snooping counters.

A higher interval reduces policy modifications and device communications.

SEE ALSO

Security Policies Overview | 2

Example: Configure DNS Snooping

SUMMARY

Read this topic to understand how to configure DNS snooping on SRX Series Firewalls to update DNS cache with mappings of FQDN and IP addresses.

IN THIS SECTION

SRX Series Firewalls support DNS snooping feature. The DNS snooping feature offers a mechanism for dynamically inspecting and caching DNS responses in real time. When you enable DNS snooping, the system captures DNS response packets as traffic traverse the network, extracting the relevant DNS records and build mapping of FQDN and IP address in a local cache. This cache provides accurate and timely DNS mappings by ensuring that IP addresses associated with Fully Qualified Domain Names (FQDNs) remain current.

TIP:

Table 34: Time Estimates

Reading Time	15 minutes
Configuration Time	30 minutes

Example Prerequisites

Table 35 on page 290 lists the hardware and software components that support the configuration.

Table 35: Requirements

Hardware requirements	SRX Series Firewalls and vSRX Virtual Firewalls
Software requirements	All SRX Series support this feature from Junos OS Release 25.2R1. We've tested this example using vSRX instances. Install and configure Application Identification. For details, see Predefined Application Signatures for Application Identification.

Before You Begin

Know more	"Configuring Security Policies" on page 96
Learn more	DNS Overview

Functional Overview

Table 36 on page 290 provides a quick summary of the configuration components deployed in this example.

Table 36: Configuration Components

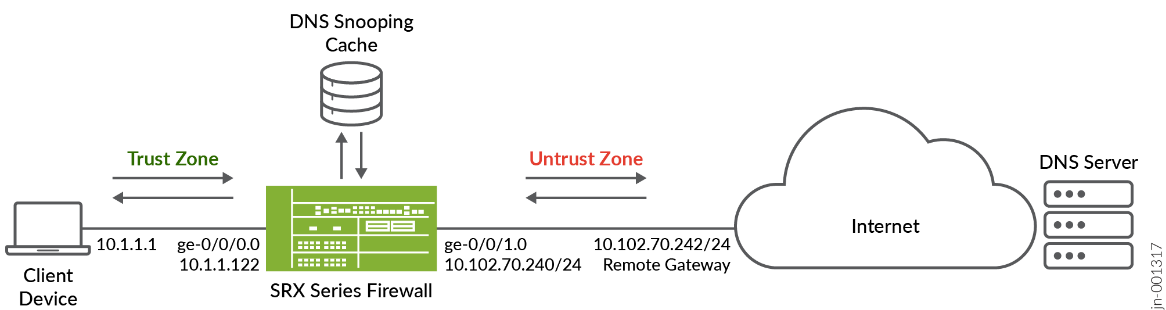
Technologies used	• Enable DNS snooping • Security zones and policies • Interfaces

Primary verification tasks	1. Verify DNS snooping cache 2. Verify DNS snooping counters

Topology Illustration

Following figure shows the topology used in this configuration example.

Figure 19: DNS Snooping Topology



In this example, the interfaces ge-0/0/0 is in the trust zone and connected to the client device (10.1.1.1). The ge-0/0/1 is in untrust zone and is connected to the DNS server through the Internet gateway (10.102.70.245). You configure DNS snooping on SRX Series Firewall.

In this example, you enable DNS snooping and create a address book with FQDN name. Then create a security policy and add the address book (FQDN name) as destination address. When the traffic matches security policy, the system captures DNS response packets as traffic traverse the network, extracting the relevant DNS records and build mapping of FQDN and IP address in a local cache. This cache provides DNS mappings by ensuring that IP addresses associated with FQDN always remain current.

Topology Overview

Table 37 on page 292 shows the details of configuration used in this example.

Table 37: Interfaces and IP Address Configuration on Security Devices

Device	Interface	IP Address	Zone	Configured For
SRX Series Firewall	ge-0/0/0.0	10.1.1.122/24	Trust	Connects to the internal client device (10.1.1.1)
	ge-0/0/0.1	10.102.70.240/24	Untrust	Connects to the Internet gateway (10.102.70.254)

Configure

To configure DNS snooping, use the following steps:

1. Enable the DNS snooping feature.

```
[edit]
user@host# set services dns-snooping
```

   Optionally you can specify trusted DNS servers to ensure that only traffic from the trusted servers is subject to DNS snooping.

```
[edit]
user@host# set services dns-snooping trusted-dns-server <server-ip-address>
```

   This configuration minimizes the risk of cache poisoning from untrusted or rogue DNS traffic. You can configure up to 32 DNS servers in a set.

2. Configure interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.102.70.240/24
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.122/24
```

3. Configure security zones.

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

```
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone untrust host-inbound-traffic system-services all
user@host# set security zones security-zone untrust host-inbound-traffic protocols all
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
```

For this example only, we have enabled host-inbound-traffic as all. Ensure you allow host inbound traffic on zones as per your network requirements.

4. Add the DNS address name as an address in the global address book and refer the address in a security policy as matching condition.

```
[edit]
user@host# set security address-book global address addr1 dns-name www.google.com
user@host# set security policies from-zone trust to-zone untrust policy p1 match source-
address any
user@host# set security policies from-zone trust to-zone untrust policy p1 match destination-
address addr1
user@host# set security policies from-zone trust to-zone untrust policy p1 match application
any
user@host# set security policies from-zone trust to-zone untrust policy p1 then permit
```

5. Apply DNS snooping to specific policy zones. This configuration restricts snooping for the traffic passing through certain zones only.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust application-services dns-
snooping
```

(Optional) You can enable DNS snooping globally.

```
[edit]
user@host# set services dns-snooping global-enable
```

You have the option to enable dns-snooping at either a zonal level or globally, but simultaneously configuring both options is not supported.

6. Configure a default policy to permit all traffic.

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

```
user@host# set security policies from-zone trust to-zone untrust policy default-permit match
destination-address any
user@host# set security policies from-zone trust to-zone untrust policy default-permit match
application any
user@host# set security policies from-zone trust to-zone untrust policy default-permit then
permit
user@host# set security policies pre-id-default-policy then log session-close
```

In this example, the default policy allows the initial traffic for the DNS lookup and then the p1 policy allows the traffic to google.com and triggers the dns-snooping.

For this example only, we have created security policies to allow all traffic. Ensure you configure security policies to restrict the traffic as per your network requirements.

Verification

IN THIS SECTION

Use the following show commands to verify the feature in this example.

Table 38: Verification Tasks

Commands	Verification Task
`show services dns-snooping cache`	Display DNS snooping counters details.
`show services dns-snooping counters`	Display DNS snooping cache information to view mapping of IP addresses associated with Fully Qualified Domain Names (FQDNs).

Check DNS Snooping Cache

Purpose

View and verify the details of DNS snooping cache.

Action

From operational mode, run the following command:

```
user@host> show services dns-snooping cache
DNS-Snooping cache on FPC: master
FQDN                             IP                        TTL
www.google.com                   142.251.46.228            242
www.google.com                   2607:f8b0:4005:813::2004 275
```

Meaning

Output displays mapping of IP address and FQDN. You can also see time-to-live (TTL) data in the output.

Check DNS Snooping Counters

Purpose

View and verify the details of DNS snooping counters.

Action

From operational mode, run the following command:

```
user@host> show services dns-snooping counters
DNS-Snooping counters on FPC:master
    Sessions ignored:           213
    Sessions interested:        85
    Sessions created:           85
    Sessions destroyed:         85
    Session dns contexts:       94
    Cache fqdn inserted:        0
```

```
    Cache fqdn deleted:          0
    Cache ip inserted:           4
    Cache ip deleted:            2
    Reports Generated:           4
    Reports Sent:                4
    Memory allocated:            102
    Memory allocation failed:    0
    Memory freed:                98
    Memory free errors:          0
    Appid errors:                0
```

Meaning

Output displays DNS snooping counter details including number of sessions processed, allocated and free memory, and AppID errors (if any).

Set Commands on All Devices

IN THIS SECTION

Set Commands on SRX Series Firewall

```
set services dns-snooping
set security address-book global address addr1 dns-name www.google.com
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 addr1
set security policies from-zone trust to-zone untrust policy p1 match application any
set security policies from-zone trust to-zone untrust policy p1 then permit
set security policies from-zone trust to-zone untrust policy default-permit match source-address
any
set security policies from-zone trust to-zone untrust policy default-permit match destination-
address any
```

```
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone trust to-zone untrust application-services dns-snooping
set security policies pre-id-default-policy then log session-close
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.122/24
set interfaces ge-0/0/1 unit 0 family inet address 10.102.70.240/24
```

Show Configuration Output

IN THIS SECTION

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

Global Address Book

```
[edit]
user@host# show security address-book
global {
    address addr1 {
```

```
        dns-name www.google.com;
    }
}
```

Services

```
[edit]
user@host# show services
dns-snooping;
```

Security Policies

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

from-zone trust to-zone untrust {
    policy p1 {
        match {
            source-address any;
            destination-address addr1;
            application any;
        }
        then {
            permit;
        }
    }
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    application-services {
        dns-snooping;
    }
```

```
}
pre-id-default-policy {
    then {
        log {
            session-close;
        }
    }
}
```

Security Zones

```
[edit]
user@host# show security zones
security-zone trust {
    tcp-rst;
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone untrust {
    screen untrust-screen;
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
```

```
    }
}
```

Interfaces

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.122/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 10.102.70.240/24;
        }
    }
}
}
```

Override Default Minimum TTL for DNS Caching

IN THIS SECTION

The NAT and policy modules use Fully Qualified Domain Names (FQDNs) from the address book for source or destination address criteria, instead of IP addresses. Upon configuration commit, these FQDNs resolve and cache results for the Time-To-Live (TTL) duration. When the TTL expires, the firewall sends query to the DNS server again.

SRX Series Firewall uses a 16-second minimum TTL for cached IP addresses. Domains with low DNS TTLs and multiple addresses are cached for 16 seconds if the TTL is under 16 seconds. This can cause IPs to be used after expiration, leading to packet drops.

Starting in Junos OS Release 25.2R1, you can override the default minimum TTL value for FQDNs in the address book. This configuration ensures DNS responses with TTL values lower or higher than 16 seconds are cached for their actual duration. This configuration overrides the default minimum TTL value of 16 seconds for FQDNs within the address book.

DNS Cache TTL Override

IN THIS SECTION

The DNS cache TTL override configuration enables you to fine-tune DNS cache behavior through the `min-ttl-override` parameter. You can override the default minimum TTL value, ensuring that DNS responses with shorter TTL values are cached for their actual duration. If the TTL is less than 16 seconds, the IP address is cached for the TTL duration; if it is exactly 16 seconds, it is cached for 16 seconds; and if greater than 16 seconds, it is cached for the specified TTL duration.

Without specific configurations, the system defaults to a caching duration of 16 seconds for TTLs less than or equal to 16 seconds, and the TTL duration for values greater than 16 seconds.

This capability allows you to cache DNS responses for their actual TTL value, even if it is lower than the default minimum. By allowing DNS responses to be cached accurately, you prevent the use of outdated addresses. This feature is particularly beneficial in environments where IP addresses change frequently, offering more accurate DNS resolution.

The system preserves default behavior for backward compatibility unless configured otherwise to ensure stability.

DNS Query Interval

Additionally, you can configure the `dns-query-interval` parameter that allows you to control the frequency of DNS queries based on received TTL values. By setting a specific interval, you ensure that DNS queries are sent at appropriate times, balancing the need for fresh DNS information with the load on DNS servers.

The DNS query interval configuration is used to forcibly send a DNS query after the configured duration, if the received TTL is more than the configured interval. Otherwise we send a DNS query after the expiry of the received TTL duration itself.

Example: If you configure the `dns-query-interval` value to be 3600 seconds and the received TTL is 4800 seconds, the system caches the entry for 3600 seconds and DNS query is sent after 3600 seconds maintaining up-to-date information without overloading the servers.

If you do not configure the `dns-query-interval`, DNS query interval is set to 84600 seconds which is equal to maximum TTL duration.

Configuration Samples

Use the following statements within the address book configuration context to override the minimum TTL for a given FQDN:

```
[edit]
user@host# set security address-book <address-book name> address <address-name> dns-name <FQDN>
min-ttl-override

user@host# set security address-book <address-book name> address <address-name> dns-name <FQDN>
dns-query-interval <value>
```

Example:

```
[edit]
user@host# set security address-book global address address-1 dns-name abc.com min-ttl-override

user@host# set security address-book global address address-1 dns-name abc.com
dns-query-interval 60
```

The above configuration ensures that DNS responses for "abc.com" with TTL values lower than 16 seconds are cached for their actual TTL duration, maintaining up-to-date IP address information.

This configuration is optional. If you do not configure `min-ttl-override`, the existing behavior continues.

You can monitoring the status of the configuration using the `show security dns-cache` command. In this example, if the received TTL is 10 seconds, the command displays following output:

```
user@host> show security dns-cache
DNS Name: google.com
 Address Family: IPv4, TTL: 1, Query Interval: 10, Override minimum TTL: Active
```

```
    IP Address: 192.168.72.206
DNS entry number: 1
```

The command output provides details such as the DNS name, address family, TTL, and whether the override is active or inactive. Use this command to verify that the configuration is applied correctly and to monitor the performance implications, ensuring that the system remains stable and optimized.

SEE ALSO

dns-name

show security dns-cache

8

CHAPTER

Security Policies for VRF-Based Traffic

IN THIS CHAPTER

Security Policies for a VRF Routing Instance

IN THIS SECTION

Overview

IN THIS SECTION

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service. A policy permits, denies, or tunnels specified types of traffic unidirectionally between two points. Security policies enforce a set of rules for transit traffic, identifying which traffic can pass through the firewall and the actions taken on the traffic as it passes through the firewall. Actions for traffic matching the specified criteria include permit and deny.

When an SRX Firewall receives a packet that matches the specifications, it performs the action specified in the policy.

Controlling Traffic in SD-WAN Architecture

In an SD-WAN, the SRX Firewall can be configured in a hub and spoke location. You can permit or deny virtual routing and forwarding (VRF) based traffic that enters the device from overlay tunnels by applying firewall policies. You can configure the SRX Firewall to permit or deny traffic that is sent to a VRF instance. Configuring the device at the hub location enables you to control all traffic at one location, and provide access to specific network services by applying firewall policies.

Each security policy consists of:

- A unique name for the policy.
- A `from-zone` and a `to-zone`, for example: `user@host# set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone`.
- A set of match criteria defining the conditions that must be satisfied to apply the policy rule. The match criteria are based on a source IP address, destination IP address, and applications. The user identity firewall provides greater granularity by including an additional tuple, such as source-identity, as part of the policy statement.
- A set of actions to be performed in case of a match—permit or deny.
- A set of source VRF group.
- A set of destination VRF group.

NOTE: The configuration options for the source and destination VRF instances are optional. You can configure either the source VRF or a destination VRF, but we recommend that you do not configure both source VRF and destination VRF. The main reason for configuring the source VRF or destination VRF is to differentiate different MPLS labels going through a shared physical network interface.

Table 39 on page 306 lists when to configure the source VRF and destination VRF.

Table 39: Recommendations for Configuring VRF Options

Network Type from Source to Destination	Recommended to Configure Source VRF	Recommended to Configure Destination VRF	VRF Policy Differentiated By
IP network to IP network	No	No	Zones
IP network to MPLS network	No	Yes	Destination VRF

Table 39: Recommendations for Configuring VRF Options *(Continued)*

Network Type from Source to Destination	Recommended to Configure Source VRF	Recommended to Configure Destination VRF	VRF Policy Differentiated By
MPLS network to IP network	Yes	No	Source VRF
MPLS network to MPLS network without destination NAT	Yes	No	Source VRF
MPLS network to MPLS network with destination NAT	Yes	Yes	Source VRF and Destination VRF

Understanding Security Policy Rules

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

Each policy is associated with the following characteristics:

- A source zone
- A destination zone
- One or many source address names or address set names
- One or many destination address names or address set names
- One or many application names or application set names
- One or many source VRF instances, for example, the VRF routing instance associated with an incoming packet
- One or many destination VRF instances in which the MPLS next hop or destination address route is located

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

You can configure either source VRF or destination VRF, but not recommended to configure both source VRF and destination VRF. The main reason for configuring source VRF and destination VR is to differentiate different MPLS labels going through a shared physical network interface. If the source VRF and destination VRF are not configured, then the device determines the source and destination VRF as any.

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

IN THIS SECTION

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF.

Requirements

- Understand how to create a security zone. See"Example: Creating Security Zones" on page 9.
- Supported SRX Firewall with any supported Junos OS Release.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.

Overview

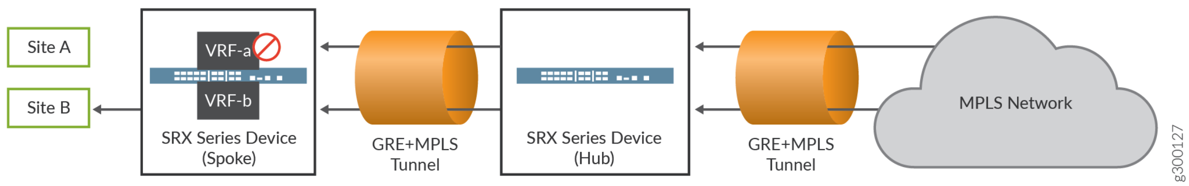
In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 20 on page 309, an SRX Firewall is deployed in an SD-WAN to control traffic using the source VRF. Traffic from the MPLS network is sent to site A and site B of the IP network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

This configuration example shows how to:

- Deny traffic to VRF-a (from GRE_Zone-GE_Zone to GRE_Zone)
- Permit traffic to VRF-b (from GRE_Zone-GE_Zone to GRE_Zone)

In this example, the source VRF is configured. We recommend that you configure the source VRF when the destination network points to the MPLS network.

Figure 20: Permitting or Denying VRF-Based Traffic from MPLS Network to an IP Network



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 routing-instances VRF-a instance-type vrf
set routing-instances VRF-a route-distinguisher 10:200
```

```
set routing-instances VRF-a vrf-target target:100:100

set routing-instances VRF-a vrf-table-label

set routing-instances VRF-b instance-type vrf

set routing-instances VRF-b route-distinguisher 20:200

set routing-instances VRF-b vrf-target target:200:100

set routing-instances VRF-b vrf-table-label

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-a_policy match source-address any

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-a_policy match destination-address any

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-a_policy match application any

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-a_policy match source-l3vpn-vrf-group  VRF-a

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-a_policy then deny

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-b_policy match source-address any

set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
```

```
vrf-b_policy match destination-address any

                    set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-b_policy match application any

                    set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-b_policy match source-l3vpn-vrf-group VRF-b

                    set security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone policy
vrf-b_policy then permit
```

Step-by-Step Procedure

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

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

   ```
   [edit routing-instances]
   user@host# set VRF-a instance-type vrf
   user@host# set VRF-b instance-type vrf
   ```

2. Assign a route distinguisher to the routing instance.

   ```
   [edit routing-instances]
   user@host# set VRF-a route-distinguisher 10:200
   user@host# set VRF-b route-distinguisher 20:200
   ```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-b vrf-table-label
```

5. Create a security policy to deny VRF-a traffic.

```
[edit security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match  source-l3vpn-vrf-group VRF-a
user@host# set policy vrf-a_policy then deny
```

6. Create a security policy to permit VRF-b traffic.

```
[edit security policies from-zone GRE_Zone-GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
```

```
user@host# set policy vrf-b_policy match source-l3vpn-vrf-group  VRF-b
user@host# set policy vrf-b_policy then permit
```

NOTE: If no destination VRF group is configured then the device considers the traffic passes from VRF-a to any-vrf.

Results

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

```
[edit]
user@host# show security policies
from-zone GRE_Zone-GE_Zone to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group VRF-a;
        }
        then {
            deny;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group VRF-b;
        }
        then {
            permit;
```

```
        }
    }
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
}
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone-GE_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source vrf: VRF-a
    destination vrf: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source vrf: VRF-b
    destination vrf: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

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

IN THIS SECTION

This example shows how to configure a security policy to permit traffic using the destination VRF.

Requirements

- Understand how to create a security zone. See "Example: Creating Security Zones" on page 9.
- Supported SRX Firewall with any supported Junos OS Release.
- Configure network interfaces on the device. See the Interfaces User Guide for Security Devices.

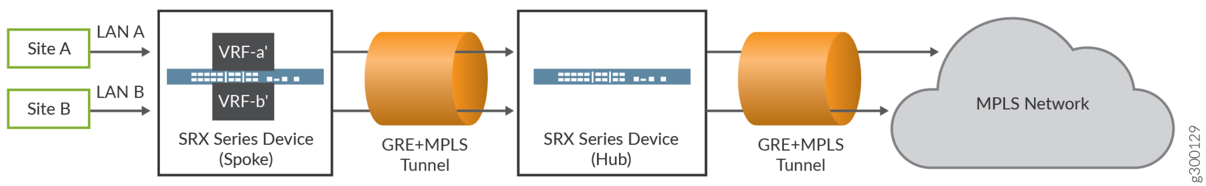
Overview

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

In this example, an SRX Firewall is deployed in an SD-WAN architecture to control traffic using the destination VRF. You need to configure policies to control the traffic. The default policy does not support VRF options. Traffic from the IP network, that is site A and site B, is sent to the MPLS network. By configuring the policies, you can permit both the traffic from site A and site B to the MPLS network.

In Figure 21 on page 316, the source VRF is not configured as the LAN interface does not belong to an MPLS network. We recommend that you configure the destination VRF when the destination network points to the MPLS network.

Figure 21: Permitting VRF-Based Traffic from an IP Network to an MPLS Network



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 routing-instances VRF-a’ instance-type vrf

                    set routing-instances VRF-a’ route-distinguisher 10:200

                    set routing-instances VRF-a’ vrf-target target:100:100

                    set routing-instances VRF-a’ vrf-table-label

                    set routing-instances VRF-b’ instance-type vrf

                    set routing-instances VRF-b’ route-distinguisher 20:200

                    set routing-instances VRF-b’ vrf-target target:200:100

                    set routing-instances VRF-b’ vrf-table-label

                    set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match source-address any

                    set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match destination-address any
```

```
                    set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match application any


                    set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match destination-l3vpn-vrf-group VRF-a'


                    set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy then permit


                    set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match source-address any


                    set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match destination-address any


                    set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match application any


                    set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match destination-l3vpn-vrf-group VRF-b'


                    set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy then permit
```

Step-by-Step Procedure

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

To configure a policy to permit traffic from the IP network to the MPLS network using the destination VRF:

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host# set VRF-a’ instance-type vrf
user@host# set VRF-b’ instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a’ route-distinguisher 10:200
user@host# set VRF-b’ route-distinguisher 20:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a’ vrf-target target:100:100
user@host# set VRF-b’ vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a’ vrf-table-label
user@host# set VRF-b’ vrf-table-label
```

5. Create a security policy to permit VRF-a’ traffic from the IP network.

```
[edit security policies from-zone LAN-a_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group VRF-a’
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit VRF-b’ traffic from the IP network.

```
[edit security policies from-zone LAN-b_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group VRF-b’
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
    from-zone LAN-a_Zone to-zone GRE_Zone {
        policy vrf-a_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                destination-l3vpn-vrf-group "VRF-a'";
```

```
            }
            then {
                permit;
            }
        }
    }
    from-zone LAN-b_Zone to-zone GRE_Zone {
        policy vrf-b_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                destination-l3vpn-vrf-group "VRF-b'";
            }
            then {
                permit;
            }
        }
    }
```

```
[edit]
user@host# show routing-instances
    VRF-a’ {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b’ {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify that the security policy permits VRF-based traffic from the IP network to the MPLS network.

Action

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

```
user@host> show security policies
From zone: LAN-a_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source vrf: any
    destination vrf: VRF-a'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: LAN-b_Zone, To zone: GRE_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source vrf: any
    destination vrf: VRF-b'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

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

IN THIS SECTION

This example shows how to configure a security policy to permit traffic using the source VRF.

Requirements

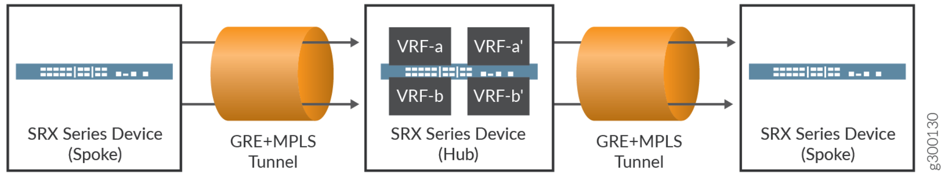
- Understand how to create a security zone. See "Example: Creating Security Zones" on page 9.
- Supported SRX Firewall with Junos OS Release 15.1X49-D160 or later. This configuration example is tested for Junos OS Release 15.1X49-D160.
- Configure network interfaces on the device. See the Interfaces User Guide for Security Devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 22 on page 324, an SRX Firewall is deployed in an SD-WAN architecture to control traffic using the source VRF. You need to configure policies to control the traffic. You can permit traffic from an MPLS network to another MPLS network by configuring policies.

We recommend that you configure both the source VRF and the destination VRF when the source and destination are from the MPLS network.

Figure 22: Permitting VRF-Based Traffic from an MPLS Network to an MPLS Network over GRE without NAT



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 routing-instances VRF-a instance-type vrf
set routing-instances VRF-a route-distinguisher 10:200
set routing-instances VRF-a vrf-target target:100:100
set routing-instances VRF-a vrf-table-label
set routing-instances VRF-b instance-type vrf
```

```
set routing-instances VRF-b route-distinguisher 20:200

set routing-instances VRF-b vrf-target target:200:100

set routing-instances VRF-b vrf-table-label

set routing-instances VRF-a’ instance-type vrf

set routing-instances VRF-a’ route-distinguisher 30:200

set routing-instances VRF-a’ vrf-target target:300:100

set routing-instances VRF-a’ vrf-table-label

set routing-instances VRF-b’ instance-type vrf

set routing-instances VRF-b’ route-distinguisher 40:200

set routing-instances VRF-b’ vrf-target target:400:100

set routing-instances VRF-b’ vrf-table-label

set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy match source-address any

set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy match destination-address any
```

```
                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy match application any


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy match source-l3vpn-vrf-group  VRF-a


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy match destination-l3vpn-vrf-group VRF-a'


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
a_policy then permit


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy match source-address any


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy match destination-address any


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy match application any


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy match source-l3vpn-vrf-group  VRF-b


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy match destination-l3vpn-vrf-group VRF-b'


                    set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-
b_policy then permit
```

Step-by-Step Procedure

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

To configure a policy to permit traffic from an MPLS network to an MPLS network using source VRF:

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host# set VRF-a instance-type vrf
user@host# set VRF-b instance-type vrf
user@host# set VRF-a' instance-type vrf
user@host# set VRF-b' instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a route-distinguisher 10:200
user@host# set VRF-b route-distinguisher 20:200
user@host# set VRF-a' route-distinguisher 30:200
user@host# set VRF-b' route-distinguisher 40:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
user@host# set VRF-a' vrf-target target:300:100
user@host# set VRF-b' vrf-target target:400:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-a' vrf-table-label
user@host# set VRF-b vrf-table-label
user@host# set VRF-b' vrf-table-label
```

5. Create a security policy to permit VRF-a traffic from the MPLS network.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-l3vpn-vrf-group VRF-a
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group VRF-a'
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit VRF-b traffic from the MPLS network.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match source-l3vpn-vrf-group VRF-b
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group VRF-b'
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
    from-zone GRE-1_Zone to-zone GRE-2_Zone {
        policy vrf-a_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                source-l3vpn-vrf-group  VRF-a;
                destination-l3vpn-vrf-group "VRF-a'";
            }
            then {
                permit;
            }
        }
        policy vrf-b_policy {
            match {
                source-address any;
                destination-address any;
                application any;
                source-l3vpn-vrf-grou  VRF-b;
                destination-l3vpn-vrf-group "VRF-b'";
            }
            then {
                permit;
            }
        }
    }
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
```

```
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
    VRF-a’ {
        instance-type vrf;
        route-distinguisher 30:200;
        vrf-target target:300:100;
        vrf-table-label;
    }
    VRF-b’ {
        instance-type vrf;
        route-distinguisher 40:200;
        vrf-target target:400:100;
        vrf-table-label;
    }
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify that the security policy permits VRF based traffic from the IP network to the MPLS network.

Action

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

```
user@host> show security policies
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-a_policy, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 1
    Source vrf: VRF-a
    destination vrf: VRF-a'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
  Policy: vrf-b_policy, State: enabled, Index: 8, Scope Policy: 0, Sequence number: 2
    Source vrf: VRF-b
    destination vrf: VRF-b'
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

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

IN THIS SECTION

This example shows how to configure security policies using VRF routing instances.

Requirements

- Supported SRX Firewall with any supported Junos OS Release.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.
- Understand how to create a security zone. See "Example: Creating Security Zones" on page 9.

Overview

In this example, you create security policies using virtual routing and forwarding (VRF) instances to isolate traffic traversing in the following networks:

- An MPLS to a private IP network
- A Global IP to an MPLS network

MPLS Network to Private IP Network

IN THIS SECTION

Procedure

Step-by-Step Procedure

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host#set VRF-a instance-type vrf
user@host#set VRF-b instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a route-distinguisher 10:200
user@host# set VRF-b route-distinguisher 20:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-b vrf-table-label
```

5. Create a security policy to permit traffic from VRF-a destined for LAN A.

```
[edit security policies from-zone GRE_Zone to-zone LAN-a_Zone]
set policy vrf-a_policy match source-address any

                        set policy vrf-a_policy match destination-address any

                        set policy vrf-a_policy match application any
```

```
set policy vrf-a_policy match source-l3vpn-vrf-group  VRF-a

set policy vrf-a_policy then permit
```

6. Create a security policy to permit traffic from VRF-b destined for LAN B.

```
[edit security policies from-zone GRE_Zone to-zone LAN-b_Zone]
set policy vrf-b_policy match source-address any

set policy vrf-b_policy match destination-address any

set policy vrf-b_policy match application any

set policy vrf-b_policy match source-l3vpn-vrf-group  VRF-b

set policy vrf-b_policy then permit
```

Results

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

```
user@host# show security policies

from-zone GRE_Zone to-zone LAN-a_Zone {
```

```
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone GRE_Zone to-zone LAN-b_Zone {

    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;

            source-l3vpn-vrf-group VRF-b;
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@host# show routing-instances
    VRF-a {
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
```

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

Global IP Network to an MPLS Network

IN THIS SECTION

Procedure

Step-by-Step Procedure

1. Layer 3 VPNs require a VRF table for distributing routes within the networks. Create a VRF instance and specify the value **vrf**.

```
[edit routing-instances]
user@host# set VRF-a instance-type vrf
user@host# set VRF-b instance-type vrf
user@host# set VRF-a' instance-type vrf
user@host# set VRF-b' instance-type vrf
```

2. Assign a route distinguisher to the routing instance.

```
[edit routing-instances]
user@host# set VRF-a route-distinguisher 10:200
user@host# set VRF-b route-distinguisher 20:200
user@host# set VRF-a' route-distinguisher 30:200
user@host# set VRF-b' route-distinguisher 40:200
```

3. Create a community policy to import or export all routes.

```
[edit routing-instances]
user@host# set VRF-a vrf-target target:100:100
user@host# set VRF-b vrf-target target:200:100
user@host# set VRF-a’ vrf-target target:300:100
user@host# set VRF-b’ vrf-target target:400:100
```

4. Assign a single VPN label for all the routes in the VRF.

```
[edit routing-instances]
user@host# set VRF-a vrf-table-label
user@host# set VRF-a’ vrf-table-label
user@host# set VRF-b vrf-table-label
user@host# set VRF-b’ vrf-table-label
```

5. Create the destination NAT pool.

```
[edit security nat destination]
user@host# set pool vrf-a_p routing-instance VRF-a
user@host# set pool vrf-a_p address 20.0.0.4/24
user@host# set pool vrf-b_p routing-instance VRF-b
user@host# set pool vrf-b_p address 30.0.0.4/24
```

6. Create a destination NAT rule set.

```
[edit security nat destination]
user@host# set rule-set rs from interface ge-0/0/0.0
user@host# set rule-set rs rule vrf-a_r match destination-address 40.0.0.4/24
user@host# set rule-set rs rule vrf-a_r then destination-nat pool vrf-a_p
```

7. Configure a rule that matches packets and translates the destination address to the address in the pool.

```
[edit security nat destination]
user@host# set rule-set rs from interface ge-0/0/1.0
user@host# set rule-set rs rule vrf-b_r match destination-address 50.0.0.4/24
user@host# set rule-set rs rule vrf-b_r then destination-nat pool vrf-b_p
```

8. Configure a security policy that allows traffic from the untrust zone to the server in the trust zone.

```
[edit security policies from-zone internet to-zone trust]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group  VRF-a’
user@host# set policy vrf-a_policy then permit
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group VRF-b’
user@host# set policy vrf-b_policy then permit
```

Results

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

```
user@host# show security policies
```

```
from-zone internet to-zone trust {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group VRF-a;

        }
        then {
            permit;
        }
    }

    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group VRF-b;
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@host# show routing-instances
    VRF-a {
```

```
        instance-type vrf;
        route-distinguisher 10:200;
        vrf-target target:100:100;
        vrf-table-label;
    }
    VRF-b {
        instance-type vrf;
        route-distinguisher 20:200;
        vrf-target target:200:100;
        vrf-table-label;
    }
    VRF-a’ {
        instance-type vrf;
        route-distinguisher 30:200;
        vrf-target target:300:100;
        vrf-table-label;
    }
    VRF-b’ {
        instance-type vrf;
        route-distinguisher 40:200;
        vrf-target target:400:100;
        vrf-table-label;
    }
```

```
user@host#
show security nat destination
pool vrf-a_p {
    routing-instance {
        VRF-a’;
    }
    address 20.0.0.4/24;
}
pool vrf-b_p {
    routing-instance {
        VRF-b’;
    }
    address 30.0.0.4/24;
}
```

```
rule-set rs {
    from interface [ ge-0/0/0.0 ge-0/0/1.0 ];
    rule vrf-a_r {
        match {
            destination-address 40.0.0.4/24;
        }
        then {
            destination-nat {
                pool {
                    vrf-a_p;
                }
            }
        }
    }
    rule vrf-b_r {
        match {
            destination-address 50.0.0.4/24;
        }
        then {
            destination-nat {
                pool {
                    vrf-b_p;
                }
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying the Destination NAT Rule

Purpose

Display information about all the destination NAT rules.

Action

From operational mode, enter the `show security nat destination rule all` command.

```
user@host> show security nat destination rule all
Total destination-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 6/0
Destination NAT rule: rule1                  Rule-set: vrf-b_r
  Rule-Id                    : 2
  Rule position              : 2
  From routing instance      : vrf-b_r
  Destination addresses      : 50.0.0.4         - 50.0.0.4
  Action                     : vrf-b_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

[...Output truncated...]

Meaning

The command displays the destination NAT rule. View the Translation hits field to check for traffic that matches the destination rule.

Verifying Flow Session

Purpose

Display information about all the currently active security sessions on the device.

Action

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

```
user@host>show security flow session
Flow Sessions on FPC0 PIC1:
Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
In: 203.0.113.11/1000  203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.1, VRF: VRF-a, Pkts: 1,
Bytes: 86, CP Session ID: 10320276
Out: 203.0.113.1/2000  203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0, VRF: VRF-b, Pkts: 0,
Bytes: 0, CP Session ID: 10320276
```

Meaning

The command displays details about all the active sessions. View the VRF field to check the VRF routing instance details in the flow.

Platform-Specific Traffic in SD-WAN Architecture Behavior

Use Feature Explorer to confirm platform and release support for specific features.

Use the following tables to review platform-specific behavior for your platform:

Platform	Difference
SRX Series	• SRX1500, SRX4100, SRX4200, SRX4600, and SRX5400 devices that support VRF-based traffic in SD-WAN architecture, support MPLS-based SDWAN deployments.

RELATED DOCUMENTATION

Flow Management in SRX Series Devices Using VRF Routing Instance

Understanding ALG Support for VRF Routing Instance

NAT for VRF Routing Instance

Security Policies Using VRF Group

IN THIS SECTION

Overview

In SD-WAN network, when different VRF based traffic enter the device from same tunnel such as GRE or GE, the device applies policy based on the given VRF instance. The device either permit or deny traffic destined to a particular VRF instance to control the VRF based traffic.

Currently, there are 5 matching conditions for each policy:

- From zone
- To zone
- Source address

- Destination address
- Applications

Figure 23 on page 345 shows the match conditions in a policy.

Figure 23: Match Conditions

	Match Conditions					Action
	From-Zone	To-Zone	SRC-Add	DST-Add	App	
P1	Z1	Z2	any	any	https	permit/UTM

g300280

With the current policy matching conditions, you cannot permit VRF-B1 or VRF-B2 and deny VRF-A1 or VRF-A2. To support this, additional matching conditions are added to the policy in the SD-WAN network using VRF group.

When the flow receives the information of source and destination VRF groups, it forwards the information to policy search API along with the policy key tuple information to meet the match conditions.

Figure 24 on page 345 shows the VRF groups added as match condition in a policy.

Figure 24: Match Conditions with VRF group

	Match Conditions							Action
	From-Zone	To-Zone	SRC-Add	DST-Add	App	source-l3vpn-vrf-group	Destination-l3vpn-vrf-group	
vpn-a_policy	GRE_Zone	GRE_Zone/GE_Zone	any	any	any	VRF-GRP_A	VRF-GRP_A'	deny
vpn-b_policy	GRE_Zone	GRE_Zone/GE_Zone	any	any	any	VRF-GRP_B	VRF-GRP_B'	permit

g300279

NOTE: If the source and destination VRF group information is not specified in a policy, then these groups matches `any` VRF group.

Example: Configuring a Security Policy to Permit VRF-Based Traffic from an IP Network to MPLS Network using VRF Group

IN THIS SECTION

This example shows how to configure a security policy to permit traffic from a private IP network to MPLs network using VRF group.

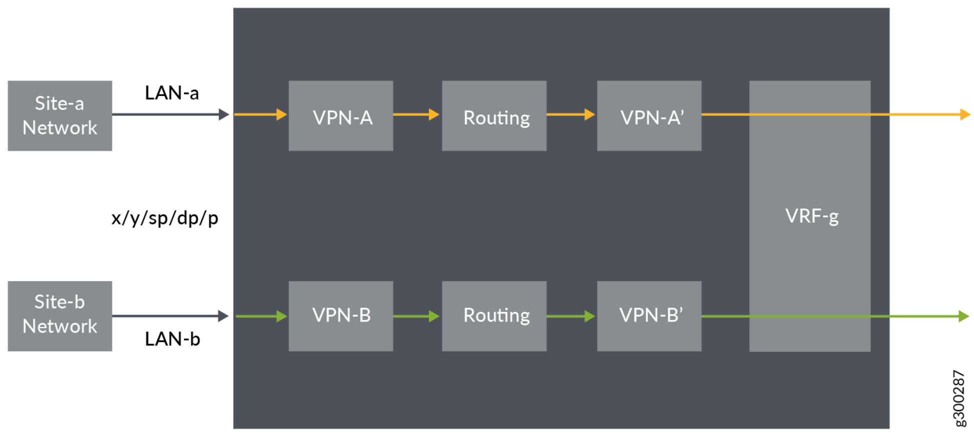
Requirements

- Any supported Junos release.
- On supported devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 25 on page 347, an SRX Series Firewall is deployed in an SD-WAN to permit the traffic from a private IP network to MPLS network using VRF group.

Figure 25: Traffic from Private Network to MPLS



This configuration example shows how to:

- Permit traffic from IP network (LAN-a) to VRF group
- Permit traffic from IP network (LAN-b) to VRF group

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-A1 vrf VRF-A11
```

```
set security l3vpn vrf-group vpn-A1 vrf VRF-A21
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security l3vpn vrf-group vpn-B1 vrf VRF-B11
set security l3vpn vrf-group vpn-B1 vrf VRF-B21
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match source-
address any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match
destination-address any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match
application any
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy match
destination-l3vpn-vrf-group vpn-A1
set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-a_policy then permit
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match source-
address any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match
destination-address any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match
application any
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy match
destination-l3vpn-vrf-group vpn-B1
set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

1. Create VRF group vpn-A with VRF instances A1 and A2

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-A1 with VRF instances A11, and A21

```
[edit security]
user@host# set l3vpn vrf-group vpn-A1 vrf VRF-A11
user@host# set l3vpn vrf-group vpn-A1 vrf VRF-A21
```

3. Create VRF group vpn-B with VRF instances B1 and B2

```
[edit security]
user@host# set l3vpn VRF group vpn-B vrf VRF-B1
user@host# set l3vpn VRF group vpn-B vrf VRF-B2
```

4. Create VRF group vpn-B1 with VRF instances B11 and B21

```
[edit security]
user@host# set l3vpn vrf-group vpn-B1 vrf VRF-B11
user@host# set l3vpn vrf-group vpn-B1 vrf VRF-B21
```

5. Create a security policy to permit vrf-a traffic.

```
[edit security policies from-zone LAN-a_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A1
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit vrf-b traffic.

```
[edit security policies from-zone LAN-a_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B1
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
from-zone LAN-a_Zone to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-VRF group vpn-A1;
        }
        then {
            permit;
        }
    }
from-zone LAN-b_Zone to-zone GRE_Zone {
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-VRF group vpn-B1;
        }
        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 security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
From zone: LAN-a_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN vrf-group: vpn-A1
    destination L3VPN VRF Group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: LAN-b_Zone, To zone: GRE_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN vrf-group: vpn-B1
    destination L3VPN VRF Group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from MPLS Network to an IP Network using VRF Group

IN THIS SECTION

This example shows how to configure a security policy to permit traffic from MPLS to IP netwrok using the VRF group.

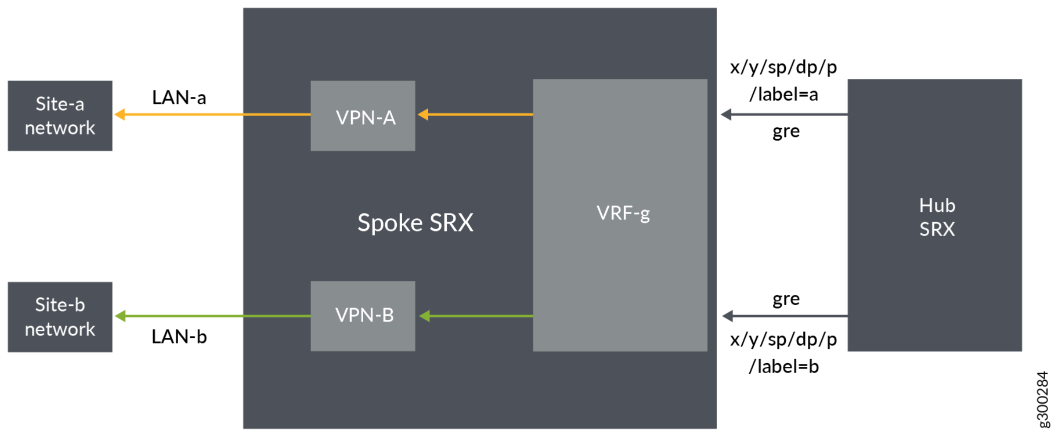
Requirements

- - Any supported Junos release.
  - On supported devices.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 26 on page 353, the firewall is deployed in an SD-WAN to permit traffic from a MPLS network to private network using VRF group.

Figure 26: Traffic Permit from MPLS to Private Network



This configuration example shows how to:

- Permit traffic from GRE MPLS to LAN-a
- Permit traffic from GRE MPLS to LAN-b

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
```

```
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security policies from-zone GRE_Zone to-zone LAN-a_Zone  policy vrf-a_policy match source-
address any
set security policies from-zone GRE_Zone to-zone LAN-a_Zone  policy vrf-a_policy match
destination-address any
set security policies from-zone GRE_Zone to-zone LAN-a_Zone  policy vrf-a_policy match
application any
set security policies from-zone GRE_Zone to-zone LAN-a_Zone  policy vrf-a_policy match source-
l3vpn-vrf-group vpn-A
set security policies from-zone GRE_Zone to-zone LAN-a_Zone  policy vrf-a_policy then permit
set security policies from-zone GRE_Zone to-zone LAN-b_Zone  policy vrf-b_policy match source-
address any
set security policies from-zone GRE_Zone to-zone LAN-b_Zone  policy vrf-b_policy match
destination-address any
set security policies from-zone GRE_Zone to-zone LAN-b_Zone  policy vrf-b_policy match
application any
set security policies from-zone GRE_Zone to-zone LAN-b_Zone  policy vrf-b_policy match source-
l3vpn-vrf-group vpn-B
set security policies from-zone GRE_Zone to-zone LAN-b_Zone  policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

1. Create VRF group vpn-A with VRF instances A1 and A2.

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-B with VRF instances B1 and B2.

```
[edit security]
user@host# set l3vpn vrf-group vpn-B vrf VRF-B1
user@host# set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Create a security policy to permit VRF-a traffic.

```
[edit security policies from-zone GRE_Zone to-zone LAN-a_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then permit
```

4. Create a security policy to permit VRF-b traffic.

```
[edit security policies from-zone GRE_Zone to-zone LAN-b_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
from-zone GRE_Zone to-zone LAN-a_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A;
        }
        then {
            permit;
        }
    }
from-zone GRE_Zone to-zone LAN-b_Zone {
    policy vrf-b_policy {
```

```
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B;
        }
        then {
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone, To zone: LAN-a_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF-Group: any
    destination L3VPN VRF Group: vpn-A
    Source addresses: any
```

```
      Destination addresses: any
      Applications: any
      Action: permit
  From zone: GRE_Zone, To zone: LAN-b_Zone
    Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
      Source L3VPN VRF Group: any
      destination L3VPN VRF-Group: vpn-B
      Source addresses: any
      Destination addresses: any
      Applications: any
      Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from Public IP Network to MPLS Network using VRF Group

IN THIS SECTION

This example describes how to configure the destination NAT rule to translate incoming public IP network to MPLS network using VRF group.

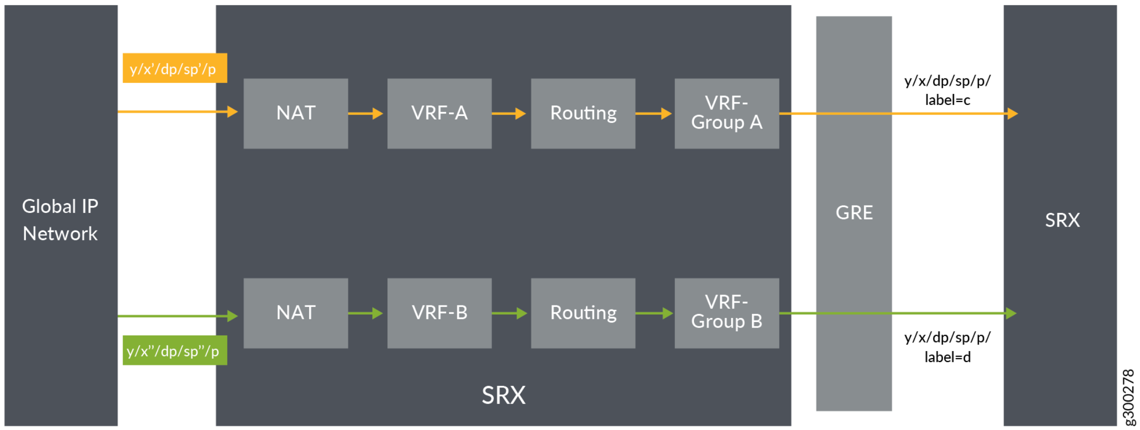
Requirements

- Understand how SRX Series Firewalls work in an SD-WAN deployment for NAT.
- Understand Virtual Routing and Forwarding Instances. See No Link Title.

Overview

In Figure 27 on page 358, the firewall is configured with destination NAT rule to translate incoming public IP network to per VRF based destination routing table and IP. The firewall is configured with two VRF groups, vpn-A and vpn-B.

Figure 27: Traffic Permit from Public Network to MPLS



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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security nat destination pool vrf-a_p routing-instance VRF-a
set security nat destination pool vrf-a_p address 192.168.1.200
```

```
set security nat destination rule-set rs from interface ge-0/0/1.0
set security nat destination rule-set rs rule vrf-a_r match destination-address 203.0.113.200
set security nat destination rule-set rs rule vrf-a_r then destination-nat pool vrf-a_p
set security nat destination pool vrf-b_p routing-instance VRF-b
set security nat destination pool vrf-b_p address 192.168.1.201
set security nat destination rule-set rs from interface ge-0/0/1.1
set security nat destination rule-set rs rule vrf-b_r match destination-address 203.0.113.201
set security nat destination rule-set rs rule vrf-b_r then destination-nat pool vrf-b_p
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-a_policy match source-
address any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-a_policy match destination-
address any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-a_policy match application
any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-a_policy match source-l3vpn-
vrf-group vpn-A
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-a_policy then permit
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-b_policy match source-
address any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-b_policy match destination-
address any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-b_policy match application
any
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-b_policy match source-l3vpn-
vrf-group vpn-B
set security policies from-zone GE_Zone to-zone GRE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

To configure destination NAT mapping for a single VRF:

1. In Layer 3 VPNs create a VRF group vpn-A with VRF instances A1 and A2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A vrf VRF-A1
user@host#set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create another VRF group vpn-B with VRF instances B1 and B2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B vrf VRF-B1
user@host#set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Specify a destination NAT IP address pool.

```
[edit security nat destination]
user@host# set pool vrf-a_p address 192.168.1.200
user@host# set pool vrf-b_p address 192.168.1.201
```

4. Assign the routing instance to the destination pool.

```
[edit security nat destination]
user@host# set pool vrf-a_p routing-instance VRF-a
user@host# set pool vrf-b_p routing-instance VRF-b
```

5. Create a destination NAT rule set.

```
[edit security nat destination]
user@host# set rule-set rs from routing-group vpn-A
user@host# set rule-set rs from routing-group vpn-B
user@host# set rule-set rs from interface ge-0/0/1.0
user@host# set rule-set rs from interface ge-0/0/1.1
```

6. Configure a rule that matches packets and translates the destination IP address to an IP address in the destination NAT IP address pool.

```
[edit security nat destination]
user@host# set rule-set rs rule vrf-a_r match destination-address 203.0.113.200
user@host# set rule-set rs rule vrf-a_r then destination-nat pool vrf-a_p
user@host# set rule-set rs rule vrf-b_r match destination-address 203.0.113.201
user@host# set rule-set rs rule vrf-b_r then destination-nat pool vrf-b_p
```

7. Create a security policy to permit VRF-a traffic.

```
[edit security policies from-zone GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then permit
```

8. Create a security policy to permit VRF-b traffic.

```
[edit security policies from-zone GE_Zone to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the `show security nat` 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# show security nat
    destination {
        pool vrf-a_p {
            routing-instance {
                VRF-a;
            }
            address 192.168.1.200/32;
        }
        pool vrf-b_p {
            routing-instance {
                VRF-b;
            }
            address 192.168.1.201/32;
        }
        rule-set rs {
```

```
            from interface [  ge-0/0/1.0 ge-0/0/1.1 ];
            rule vrf-a_r {
                match {
                    destination-address 203.0.113.200/32;
                }
                then {
                    destination-nat {
                        pool {
                            vrf-a_p;
                        }
                    }
                }
            }
            rule vrf-b_r {
                match {
                    destination-address 203.0.113.201/32;
                }
                then {
                    destination-nat {
                        pool {
                            vrf-b_p;
                        }
                    }
                }
            }
        }
    }
```

```
[edit]
user@host# show security policies
from-zone GE_Zone to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A;
        }
        then {
            permit;
        }
```

```
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B;
        }
        then {
            permit;
        }
    }
```

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

Verification

IN THIS SECTION

Verifying Destination NAT Rule Usage and Security Policies

Purpose

Verify that there is traffic matching the destination NAT rule.

Action

From operational mode, enter the `show security nat destination rule all` command. In the Translation hits field, verify whether there is traffic that matches the destination NAT rule.

```
user@host> show security nat destination rule all
Total destination-nat rules: 2
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Destination NAT rule: vrf-a_r                Rule-set: rs
  Rule-Id                    : 1
  Rule position              : 1
  From interface                  : ge-0/0/1.0
```

```
  Destination addresses      : 203.0.113.200   - 203.0.113.200
  Action                     : vrf-a_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
    Destination NAT rule         : vrf-b_r
  Rule-set                                     : rs
  Rule-Id                    : 2
  Rule position              : 2
  From interface             : ge-0/0/1.1
  Destination addresses      : 203.0.113.201   - 203.0.113.201
  Action                     : vrf-b_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

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

```
user@root> show security policies
Default policy: permit-all
From zone: GE_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: any
    destination L3VPN VRF-Group: vpn-A
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: GE_Zone, To zone: GRE_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: any
    destination L3VPN VRF-Group: vpn-B
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from MPLS Network to Public IP Network to using VRF Group

IN THIS SECTION

This example describes how to configure the routing group to translate per VRF group network traffic to global IP pool.

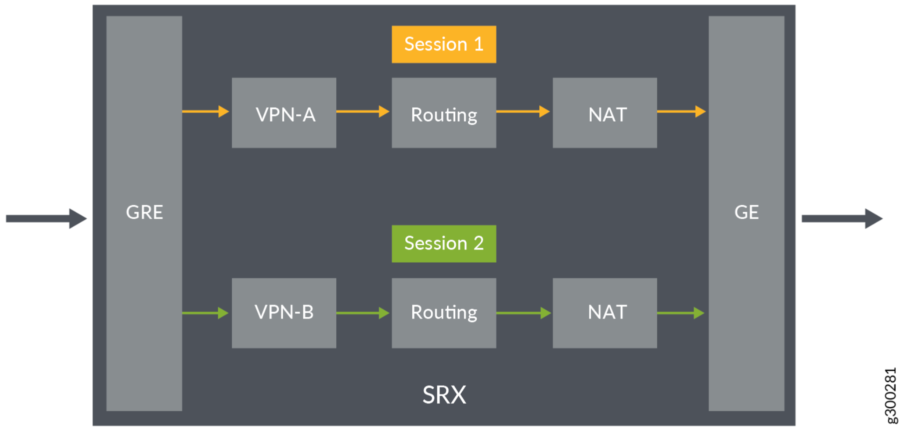
Requirements

- Understand how the firewall work in an SD-WAN deployment for NAT.
- Understand Virtual Routing and Forwarding Instances. See No Link Title.

Overview

In Figure 28 on page 366, the firewall is configured with routing group to permit VRF group network traffic from MPLS to global IP pool. The firewall is configured with two VRF groups, vpn-A and vpn-B.

Figure 28: Traffic Permit from MPLS to Public Network



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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security nat source pool vrf-a_p address 203.0.113.200
set security nat source rule-set vrf-a_rs from routing-group vpn-A
```

```
set security nat source rule-set vrf-a_rs to zone GE_Zone
set security nat source rule-set vrf-a_rs rule rule1 match source-address 192.168.1.200
set security nat source rule-set vrf-a_rs rule rule1 then source-nat pool vrf-a_p
set security nat source pool vrf-b_p address 203.0.113.201
set security nat source rule-set vrf-b_rs from routing-group vpn-B
set security nat source rule-set vrf-b_rs to zone GE_Zone
set security nat source rule-set vrf-b_rs rule rule2 match source-address 192.168.1.201
set security nat source rule-set vpn-b_rs rule rule2 then source-nat pool vrf-b_p
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-a_policy match source-
address any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-a_policy match destination-
address any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-a_policy match application
any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-a_policy match source-l3vpn-
vrf-group vpn-A
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-a_policy then permit
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-b_policy match source-
address any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-b_policy match destination-
address any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-b_policy match application
any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-b_policy match source-l3vpn-
vrf-group vpn-B
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

To configure source NAT mapping for a single VRF:

1. In Layer 3 VPNs create a VRF group vpn-A with VRF instances A1 and A2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A vrf VRF-A1
user@host#set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create another VRF group vpn-B with VRF instances B1 and B2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B vrf VRF-B1
user@host#set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Specify a source NAT IP address pool.

```
[edit security nat source]
user@host# set pool vrf-a_p address 192.168.1.200
user@host# set pool vrf-b_p address 192.168.1.201
```

4. Create a source NAT rule set.

```
[edit security nat source]
user@host# set rule-set rs from routing-group vpn-A
user@host# set rule-set rs from routing-group vpn-B
user@host# set rule-set rs to zone GE_Zone
```

5. Configure a rule that matches packets and translates per VRF group network traffic to global IP pool.

```
[edit security nat source]
user@host# set rule-set rs rule vrf-a_r match destination-address 203.0.113.200
user@host# set rule-set rs rule vrf-a_r then destination-nat pool vrf-a_p
user@host# set rule-set rs rule vrf-b_r match destination-address 203.0.113.201
user@host# set rule-set rs rule vrf-b_r then destination-nat pool vrf-b_p
```

6. Create a security policy to permit vpn-A traffic.

```
[edit security policies from-zone GRE_Zone to-zone GE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then permit
```

7. Create a security policy to permit vpn-B traffic.

```
[edit security policies from-zone GRE_Zone to-zone GE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the `show security nat` 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# show security nat
    source {
        pool vrf-a_p {
            address {
                203.0.113.200/32;
            }
        }
        pool vrf-b_p {
            address {
                203.0.113.201/32;
            }
        }
        rule-set vrf-a_rs {
            from routing-group vpn-A;
            to zone GE_Zone1;
            rule rule1 {
                match {
                    source-address 192.168.1.200/32;
                }
                then {
                    source-nat {
                        pool {
                            vrf-a_p;
                        }
                    }
```

```
                }
            }
            rule-set vrf-b_rs {
                from routing-group vpn-B;
                to zone GE_Zone;
                match {
                    source-address 192.168.1.201/32;
                }
                then {
                    source-nat {
                        pool {
                            vrf-b_p;
                        }
                    }
                }
            }
        }
    }
```

```
[edit]
user@host# show security policies
from-zone GRE_Zone to-zone GE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A;
        }
        then {
            permit;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B;
        }
        then {
```

```
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Destination NAT Rule Usage and Security Policies

Purpose

Verify that there is traffic matching the source NAT rule.

Action

From operational mode, enter the `show security nat source rule all` command. In the Translation hits field, verify whether there is traffic that matches the source NAT rule.

```
user@host> show security nat source rule all
Total source-nat rules: 2
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Source NAT rule                        : vrf-a_r
Rule-set: rs
  Rule-Id                    : 1
  Rule position              : 1
  From routing-group         : vpn-A  To zone                     : GE_Zone1
  Source addresses               : 203.0.113.200   - 203.0.113.200
  Action                     : vrf-a_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
Source NAT rule                         : vrf-b_r
```

```
Rule-set: rs
  Rule-Id                    : 2
  Rule position              : 2
  From routing-group         : vpn-A
  To zone                    : GE_Zone
  Destination addresses      : 203.0.113.201   - 203.0.113.201
  Action                     : vrf-b_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

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

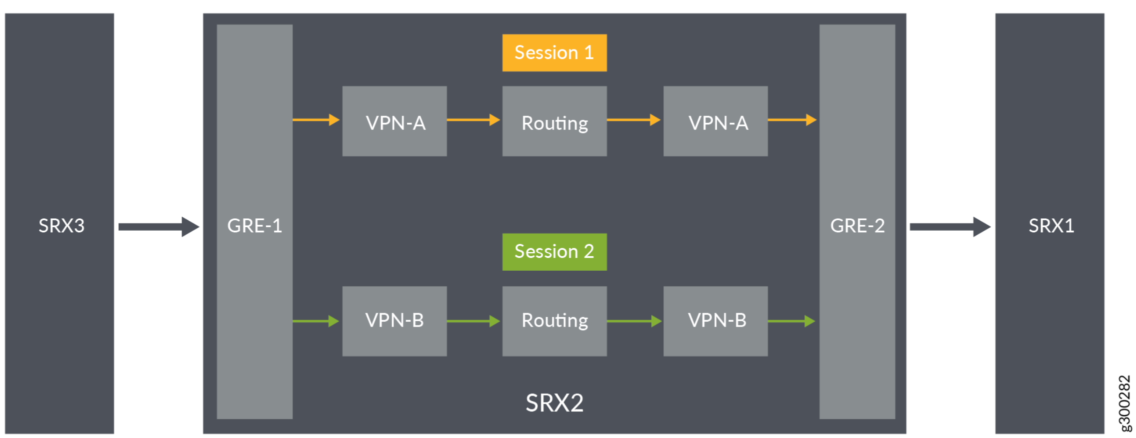
```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone, To zone: GE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: any
    destination L3VPN VRF Group: vpn-A
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: GRE_Zone, To zone: GE_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: any
    destination L3VPN VRF Group: vpn-B
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from MPLS Network to MPLS Network without NAT using VRF Group

IN THIS SECTION

This example describes how to configure the routing group to permit traffic between MPLS networks without using NAT.

Figure 29: Traffic between MPLS Networks



Requirements

- Understand how the firewall work in an SD-WAN deployment for NAT.
- Understand Virtual Routing and Forwarding Instances. See No Link Title.

Overview

In Figure 29 on page 373, the firewall is configured with routing group to permit traffic between MPLS networks without using NAT. The firewall is configured with two VRF groups, vpn-A and vpn-B.

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-A1 vrf VRF-A11
set security l3vpn vrf-group vpn-A1 vrf VRF-A12
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security l3vpn vrf-group vpn-B1 vrf VRF-B11
set security l3vpn vrf-group vpn-B1 vrf VRF-B12
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-
address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match
destination-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match
application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-
l3vpn-vrf-group vpn-A1
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy then permit
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-
address any
```

```
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match
destination-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match
application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-
l3vpn-vrf-group vpn-B1
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

To configure source NAT mapping for a single VRF:

1. In Layer 3 VPNs create a VRF group vpn-A with VRF instances A1and A2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A vrf VRF-A1
user@host#set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. In Layer 3 VPNs create a VRF group vpn-A1 with VRF instances A11and A12.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A1 vrf VRF-A11
user@host#set l3vpn vrf-group vpn-A1 vrf VRF-A12
```

3. Create another VRF group vpn-B with VRF instances B1 and B2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B vrf VRF-B1
user@host#set l3vpn vrf-group vpn-B vrf VRF-B2
```

4. Create another VRF group vpn-B1 with VRF instances B11 and B12.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B1 vrf VRF-B11
user@host#set l3vpn vrf-group vpn-B1 vrf VRF-B12
```

5. Create a security policy to permit vpn-A1 traffic.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A1
user@host# set policy vrf-a_policy then permit
```

6. Create a security policy to permit vpn-B1 traffic.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B1
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
from-zone GRE-1_Zone to-zone GRE-2_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A1;
```

```
        }
        then {
            permit;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B1;
        }
        then {
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Security Policies

Purpose

Verify that configuration output of security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
```

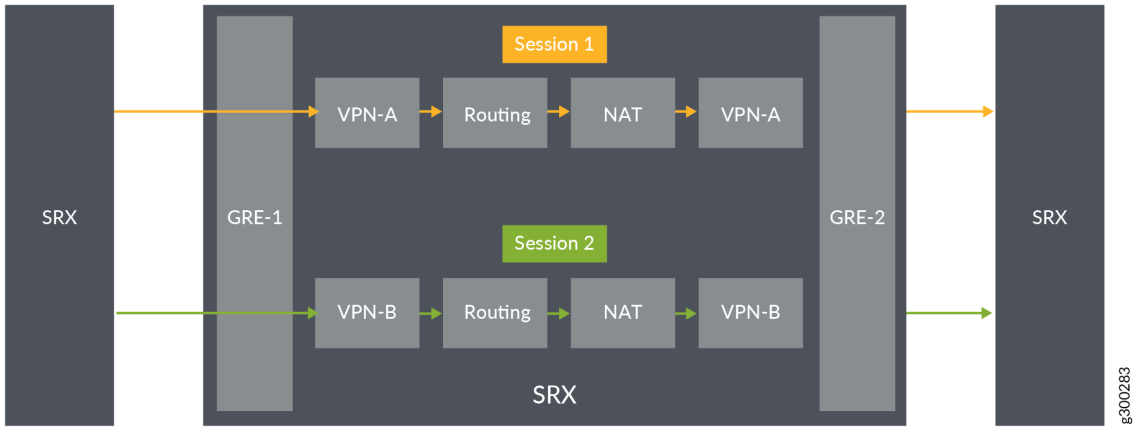
```
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: any
    destination L3VPN VRF-Group: vpn-A1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: any
    destination L3VPN VRF-Group: vpn-B1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Example: Configuring a Security Policy to Permit VRF-Based Traffic from MPLS Network to MPLS Network using NAT and VRF Group

IN THIS SECTION

This example describes how to configure the routing group and permit traffic between MPLS networks using NAT.

Figure 30: Traffic Permit between MPLS Networks with NAT



Requirements

- Understand how SRX Series Firewalls work in an SD-WAN deployment for NAT.
- Understand Virtual Routing and Forwarding Instances. See No Link Title.

Overview

In Figure 30 on page 379, an SRX Series Firewall is configured the routing group and permit traffic between MPLS networks using NAT. The SRX Series Firewall is configured with the VRF groups, vpn-A, vpn-A1, vpn-B, and vpn-B1.

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-A1 vrf VRF-A11
set security l3vpn vrf-group vpn-A1 vrf VRF-A12
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security l3vpn vrf-group vpn-B1 vrf VRF-B11
set security l3vpn vrf-group vpn-B1 vrf VRF-B12
set security nat source pool vrf-a_p address 203.0.113.200
set security nat source rule-set vrf-a_rs from routing-group vpn-A
set security nat source rule-set vrf-a_rs to routing-group vpn-A1
set security nat source rule-set vrf-a_rs rule rule1 match source-address 192.168.1.200
set security nat source rule-set vrf-a_rs rule rule1 then source-nat pool vrf-a_p
set security nat source pool vrf-b_p address 203.0.113.201
set security nat source rule-set vrf-b_rs from routing-group vpn-B
set security nat source rule-set vrf-b_rs to routing-group vpn-B1
set security nat source rule-set vrf-b_rs rule rule2 match source-address 192.168.1.201
set security nat source rule-set vrf-b_rs rule rule2 then source-nat pool vrf-b_p
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-
address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match
destination-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match
application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy match source-
l3vpn-vrf-group vpn-A1
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-a_policy then permit
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-
address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match
destination-address any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match
application any
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy match source-
```

```
l3vpn-vrf-group vpn-B1
set security policies from-zone GRE-1_Zone to-zone GRE-2_Zone policy vrf-b_policy then permit
```

Step-by-Step Procedure

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

To configure source NAT mapping for a single VRF:

1. In Layer 3 VPNs create a VRF group vpn-A with VRF instances A1and A2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A vrf VRF-A1
user@host#set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. In Layer 3 VPNs create a VRF group vpn-A1 with VRF instances A11and A12.

```
[edit security]
user@host#set l3vpn vrf-group vpn-A1 vrf VRF-A11
user@host#set l3vpn vrf-group vpn-A1 vrf VRF-A12
```

3. Create another VRF group vpn-B with VRF instances B1 and B2.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B vrf VRF-B1
user@host#set l3vpn vrf-group vpn-B vrf VRF-B2
```

4. Create another VRF group vpn-B1 with VRF instances B11 and B12.

```
[edit security]
user@host#set l3vpn vrf-group vpn-B1 vrf VRF-B11
user@host#set l3vpn vrf-group vpn-B1 vrf VRF-B12
```

5. Specify a source NAT IP address pool.

```
[edit security nat source]
user@host# set pool vrf-a_p address 192.168.1.200
user@host# set pool vrf-b_p address 192.168.1.201
```

6. Create a source NAT rule set.

```
[edit security nat source]
user@host# set rule-set rs from routing-group vpn-A
user@host# set rule-set rs from routing-group vpn-B
user@host# set rule-set rs to routing-group vpn-A1
user@host# set rule-set rs to routing-group vpn-B1
```

7. Configure a rule that matches packets and translates per VRF group network traffic to global IP pool.

```
[edit security nat source]
user@host# set rule-set rs rule vrf-a_rs match destination-address 203.0.113.200
user@host# set rule-set rs rule vrf-a_rs then destination-nat pool vrf-a_p
user@host# set rule-set rs rule vrf-b_rs match destination-address 203.0.113.201
user@host# set rule-set rs rule vrf-b_rs then destination-nat pool vrf-b_p
```

8. Create a security policy to permit vpn-A1 traffic.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A1
user@host# set policy vrf-a_policy then permit
```

9. Create a security policy to permit vpn-B1 traffic.

```
[edit security policies from-zone GRE-1_Zone to-zone GRE-2_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
```

```
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B1
user@host# set policy vrf-b_policy then permit
```

Results

From configuration mode, confirm your configuration by entering the `show security nat` 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# show security nat
    source {
        pool vrf-a_p {
            address {
                203.0.113.200/32;
            }
        }
        pool vrf-b_p {
            address {
                203.0.113.201/32;
            }
        }
        rule-set vrf-a_rs {
            from routing-group vpn-A;
            to routing-group vpn-A1;
            rule rule1 {
                match {
                    source-address 192.168.1.200/32;
                }
                then {
                    source-nat {
                        pool {
                            vrf-a_p;
                        }
                    }
                }
            }
            rule-set vrf-b_rs {
                from routing-group vpn-B;
                to routing-group vpn-B1;
```

```
                match {
                    source-address 192.168.1.201/32;
                }
                then {
                    source-nat {
                        pool {
                            vrf-b_p;
                        }
                    }
                }
            }
        }
    }
```

```
[edit]
user@host# show security policies
from-zone GRE-1_Zone to-zone GRE-2_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A1;
        }
        then {
            permit;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B1;
        }
        then {
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Security Policies

Purpose

Verify that there is traffic matching the source NAT rule.

Action

From operational mode, enter the `show security nat source rule all` command. In the Translation hits field, verify whether there is traffic that matches the destination NAT rule.

```
user@host> show security nat source rule all
Total source-nat rules: 2
Total referenced IPv4/IPv6 ip-prefixes: 2/0
Source NAT rule                        : vrf-a_r
Rule-set                                         : rs
  Rule-Id                    : 1
  Rule position              : 1
  From routing-group         : vpn-A
  To zone                    : GE_Zone1
  Source addresses               : 203.0.113.200   - 203.0.113.200
  Action                     : vrf-a_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
Source NAT rule                        : vrf-b_r
 Rule-set                                     : rs
  Rule-Id                    : 2
  Rule position              : 2
  From routing-group         : vpn-A
```

```
  To zone                    : GE_Zone
  Destination addresses      : 203.0.113.201   - 203.0.113.201
  Action                     : vrf-b_p
  Translation hits           : 0
    Successful sessions      : 0
    Failed sessions          : 0
  Number of sessions         : 0
```

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

```
user@root> show security policies
Default policy: permit-all
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: any
    destination L3VPN VRF Group: vpn-A1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
From zone: GRE-1_Zone, To zone: GRE-2_Zone
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: any
    destination L3VPN VRF Group: vpn-B1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

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

IN THIS SECTION

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF group.

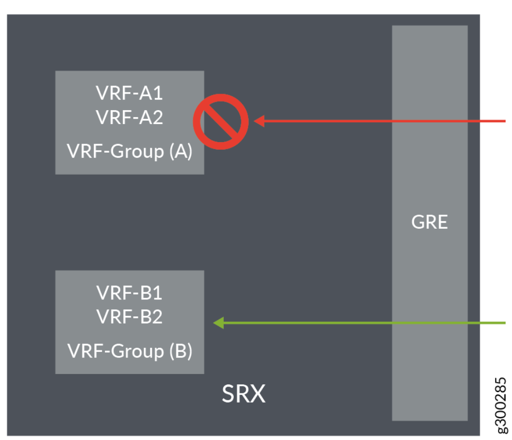
Requirements

- Understand how to create a security zone. See "Example: Creating Security Zones" on page 9 .
- Supported SRX Firewall with any supported Junos OS Release.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 31 on page 387, an SRX Firewall is deployed in an SD-WAN to control traffic using the source VRF group. Traffic from the GRE MPLS network is sent to site A and site B of the IP network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

Figure 31: Policy Control from MPLS network



This configuration example shows how to:

- Deny traffic from vpn-A (from GRE MPLS)
- Permit traffic from vpn-B (from GRE MPLS)

Configuration

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
set security l3vpn vrf-group vpn-B vrf VRF-B1
set security l3vpn vrf-group vpn-B vrf VRF-B2
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
a_policy match source-address any
set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
a_policy match destination-address any
```

```
                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
a_policy match application any

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
a_policy match source-l3vpn-vrf-group vpn-A

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
a_policy then deny

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
b_policy match source-address any

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
b_policy match destination-address any

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
b_policy match application any

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
b_policy match source-l3vpn-vrf-group vpn-B

                    set security policies from-zone GRE_Zone to-zone GE_Zone policy vrf-
b_policy then permit
```

Step-by-Step Procedure

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

1. Create VRF group vpn-A with VRF instances A1 and A2

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-B with VRF instances B1 and B2

```
[edit security]
user@host# set l3vpn vrf-group vpn-B vrf VRF-B1
user@host# set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Create a security policy to deny vpn-A traffic.

```
[edit security policies from-zone GRE_Zone to-zone GE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match source-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then deny
```

4. Create a security policy to permit vpn-B traffic.

```
[edit security policies from-zone GRE_Zone to-zone GE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match source-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
from-zone GRE_Zone to-zone GE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group vpn-A;
        }
        then {
            deny;
        }
    }
    policy vrf-b_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            source-l3vpn-vrf-group vpn-B;
        }
        then {
            permit;
        }
    }
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
From zone: GRE_Zone, To zone: GE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: vpn-A
    destination L3VPN vrf-group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny
  Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: vpn-B
    destination L3VPN vrf-group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

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

IN THIS SECTION

This example shows how to configure a security policy to permit traffic and deny traffic using the source VRF group.

Requirements

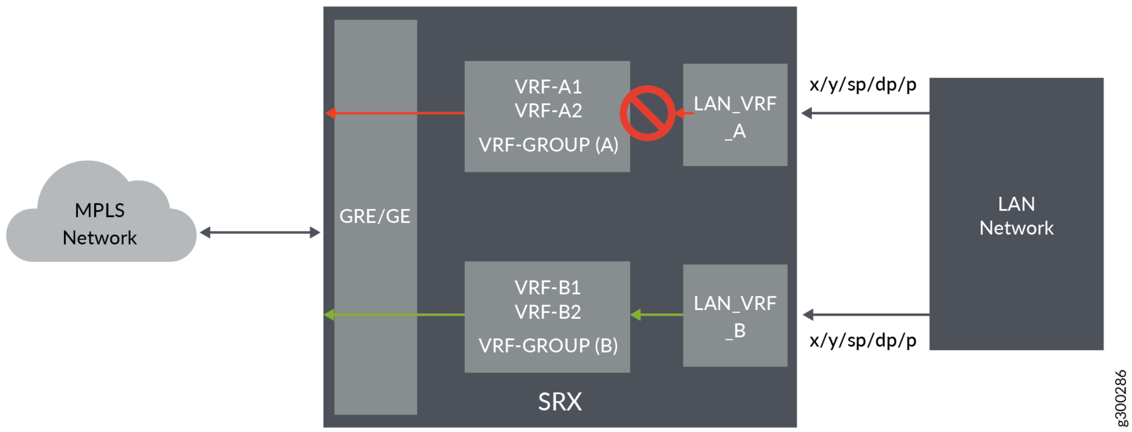
- Understand how to create a security zone. See "Example: Creating Security Zones" on page 9.
- Supported SRX Firewall with any supported Junos OS Release.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. In Figure 32 on page 394, an SRX Firewall is deployed in an SD-WAN to control traffic using the destination VRF group. Traffic from IP network is sent to site A and site B of the GRE MPLS network. As per the network requirement, site A traffic should be denied, and only site B traffic should be permitted.

This configuration example shows how to:

Figure 32: Policy control to MPLS network



- Deny traffic to vpn-A (to GRE MPLS)
- Permit traffic to vpn-B (to GRE MPLS)

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 l3vpn vrf-group vpn-A vrf VRF-A1
set security l3vpn vrf-group vpn-A vrf VRF-A2
```

```
set security l3vpn vrf-group vpn-B vrf VRF-B1

set security l3vpn vrf-group vpn-B vrf VRF-B2

set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match source-address any

set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match destination-address any

set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match application any

set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy match destination-l3vpn-vrf-group vpn-A

set security policies from-zone LAN-a_Zone to-zone GRE_Zone policy vrf-
a_policy then deny

set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match source-address any

set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match destination-address any

set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match application any

set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy match destination-l3vpn-vrf-group vpn-B
```

```
            set security policies from-zone LAN-b_Zone to-zone GRE_Zone policy vrf-
b_policy then permit
```

Step-by-Step Procedure

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

1. Create VRF group vpn-A with VRF instances A1 and A2

```
[edit security]
user@host# set l3vpn vrf-group vpn-A vrf VRF-A1
user@host# set l3vpn vrf-group vpn-A vrf VRF-A2
```

2. Create VRF group vpn-B with VRF instances B1 and B2

```
[edit security]
user@host# set l3vpn vrf-group vpn-B vrf VRF-B1
user@host# set l3vpn vrf-group vpn-B vrf VRF-B2
```

3. Create a security policy to deny vpn-A traffic.

```
[edit security policies from-zone LAN-a_Zone  to-zone GRE_Zone]
user@host# set policy vrf-a_policy match source-address any
user@host# set policy vrf-a_policy match destination-address any
user@host# set policy vrf-a_policy match application any
user@host# set policy vrf-a_policy match destination-l3vpn-vrf-group vpn-A
user@host# set policy vrf-a_policy then deny
```

4. Create a security policy to permit vpn-B traffic.

```
[edit security policies from-zone LAN-b_Zone e to-zone GRE_Zone]
user@host# set policy vrf-b_policy match source-address any
user@host# set policy vrf-b_policy match destination-address any
user@host# set policy vrf-b_policy match application any
user@host# set policy vrf-b_policy match destination-l3vpn-vrf-group vpn-B
user@host# set policy vrf-b_policy then permit
```

Results

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

```
[edit]
user@host# show security policies
from-zone LAN-a_Zone  to-zone GRE_Zone {
    policy vrf-a_policy {
        match {
            source-address any;
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-A;
        }
        then {
            deny;
        }
    }
}
    from-zone LAN-b_Zone  to-zone GRE_Zone {
    policy vrf-b_policy {
        match {
            source-address any;
```

```
            destination-address any;
            application any;
            destination-l3vpn-vrf-group vpn-B;
        }
        then {
            permit;
        }
    }
}
```

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

Verification

IN THIS SECTION

Verifying Policy Configuration

Purpose

Verify information about security policies.

Action

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

```
user@root> show security policies
Default policy: permit-all
From zone:  LAN-a_Zone, To zone: GRE_Zone
  Policy: vrf-a_policy, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source L3VPN VRF Group: any
    destination L3VPN vrf-group: vpn-A
    Source addresses: any
    Destination addresses: any
    Applications: any
```

```
    Action: deny
 From zone:  LAN-b_Zone, To zone: GRE_Zone
    Policy: vrf-b_policy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source L3VPN VRF Group: any
    destination L3VPN vrf-group: vpn-B
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: permit
```

Managing Overlapping VPN using VRF group

When there are two sessions in a L3VPN network, to avoid any conflicts between the two sessions VRF group-ID is added to session key as an additional key to differentiate the sessions.

In Figure 33 on page 399 network1 and network3 are grouped together to VRF group-A in L3VPN network, and network2 and network4 are grouped together to VRF group-B. The sessions use VRF group-A and VRF group-B as differentiators.

Figure 33: Overlapping VPN using VRF groups

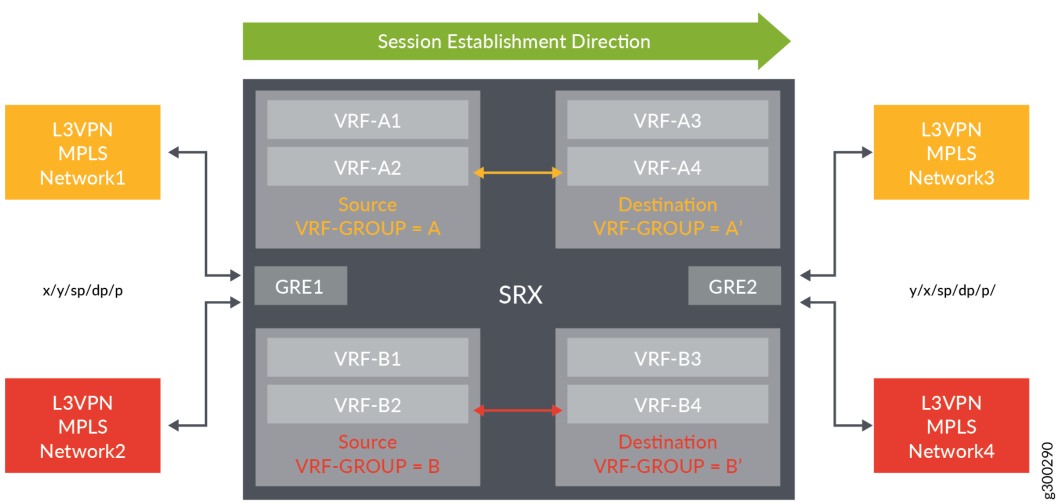


Table 40 on page 400

Table 40: L3VPN Session Information

L3VPN Network 1 and 3 session		L3VPN Network 2 and 4 session	
(Forward)	(Reverse)	(Forward)	(Reverse)
5-tuple: x/y/sp/dp/p	5-tuple: y/x/dp/sp/p	5-tuple: x/y/sp/dp/p	5-tuple: y/x/dp/sp/p
Token: GRE1(zone_id +VR_id) + VRF group-ID (A)	Token: GRE1(zone_id +VR_id) + VRF group-ID (B)	Token: GRE1(zone_id +VR_id) + VRF group-ID (A')	Token: GRE1(zone_id +VR_id) + VRF group-ID (B')

RELATED DOCUMENTATION

Flow Processing using Virtual Routing and Forwarding Group

Security Policies with VRF-Aware Security Zones

IN THIS SECTION

VRF-Aware Zone-Based Policy Enforcement

IN THIS SECTION

Overview

The VRF-aware zone-based policy enforcement feature introduces a strategic approach to managing security policies at the VRF level.

You can now create zones for each VRF instance and apply policies between VRF instances to simplify Layer 3 VPN (L3VPN) policy management for MPLS and VXLAN. By defining VRF-aware security zones, you gain a more granular level of control of both intra-VRF and inter-VRF traffic and control across L3VPN deployments. The policy lookup process adapts to integrate VRF-based zones alongside interface-based zones, allowing comprehensive policy enforcement.

You define security zones by VRF instance (not by VRF group). The VRF-group restriction in the policy rule set remains unchanged. For incoming traffic, the firewall evaluates the L3VPN zone first, and then the physical interface zone; if no zone matches, the firewall drops packets.

Configure security zones per VRF using the `vrf` option under the `[edit security zones security-zone *zone-name*]` hierarchy level. Verify your configuration using the `show security policies` and `show security zones` operational commands. These commands display the VRF-based zone names in the existing syslog's `source-zone-name` and `destination-zone-name` fields. Also, new syslog fields, `src-vrf` and `dst-vrf`, display the source and destination VRF instances. See System Log Explorer | Juniper Networks Pathfinder.

VRF-Aware Zone-Based Security Policies

Previously, zone changes were handled in a single-level zone model, and any change in the zone would tear down the session entirely.

Overview

You can now define zones using VRF instances (VRF-aware zones), similar to how you define zones with interfaces. The policy lookup process incorporates VRF zones, enabling cross-combinations with interface-based zones for comprehensive policy enforcement.

Define zones using VRF instances: VRF-aware zones behave the same way as interface-based zone contexts when it comes to policy evaluation. Similar to how interface-based *from zone* and *to zone* combinations are considered as contexts, VRF zones are considered the same way. The firewall flow sends the VRF zones to the policy in the same way as it sends interface zone details for policy lookup.

We now support two-level zones, where MPLS and VXLAN traffic are matched within VRF-specific zones. This approach ensures that sessions are governed by VRF-specific policies without affecting other overlay or underlay zones.

Traffic evaluation (based on type):

- For MPLS or VXLAN traffic, the highest priority is given to VRF-based zones.
- For IP traffic, the device checks only interface-based zones.

Policy evaluation (based on traffic type):

- For MPLS and VXLAN traffic, policy evaluation uses VRF-based zones.
- For IP traffic, policy evaluation uses only interface-based zones.

  The single VRF-group policy limitation remains to prevent ambiguous matches.

VRF-aware zones and interface-based zones remain segregated; VRF-aware zones cannot include interfaces; interface zones cannot reference VRF-aware zones.

> **NOTE**: VRF-aware zone-based policy enforcement is backward compatible, ensuring that existing VRF-level enforcement remains functional while incorporating new VRF-based zone configurations.
> To maintain backward compatibility, configuring both VRF-based zone and VRF match criteria in the same policy is not supported, and doing so results in a commit error.

For MPLS and VXLAN traffic, sessions are created based on the VRF-specific zone policies. Packets are matched against the VRF zone, and if a match occurs, the device establishes a session accordingly.

Flow Session Behavior

This section describes the behavior of flow sessions across three scenarios: overlay-to-overlay, underlay-to-underlay, and overlay-to-underlay flows.

You can manage zone and VRF changes with predictable session behavior to maintain traffic continuity.

If the traffic is matched to an overlay zone, then the sessions do not terminate when you add an interface to an underlay zone or delete an unused interface. The device also preserves traffic when you add a VRF instance to the traffic-matched overlay zone or delete an unused VRF instance from that overlay zone.

If the traffic is matched to an overlay zone, then the sessions terminate when you rename the underlay zone or delete the interface carrying overlay-zone-matched traffic in the underlay zone.

Configuration Overview

VRF-based zones are exclusive to VRF instances and do not support direct interface configurations, similarly interface-based zones do not accommodate VRF instances. Virtual network identifier (VNI)-aware zones are not supported.

Configure VRF zones: Define VRF zones and associate them with specific policies using the CLI, Security Director, or Security Director Cloud.

Verify VRF zones configuration: Use the existing policy and zone show commands. The command outputs are now updated to include VRF zone details, granting visibility into the current configurations and any potential discrepancies.

VRF-Aware Zone-Based Policy Configuration Limitations

- You can configure zones only based on a VRF instance and not based on a VRF group.
- For each VRF instance, choose either VRF group or a VRF zone; configuring both causes a commit failure, generating a commit error.
- Traffic between VRF group and a VRF zone is not permitted. Flow processing explicitly denies and drops any traffic between a VRF group and a VRF zone.
- Configuring interfaces and VRF instances under the same zone results in a commit error as show below:

```
user@host#  commit
[edit security zones security-zone vrf-zone1]
  'vrf'
    vrf and interfaces cannot be configured together
 error: commit failed: (statements constraint check failed)
 [edit]
```

- Configuring both VRF-based zone and VRF match criteria in the same policy results in a commit error as shown below:

```
user@host#  commit
[edit security policies from-zone trust to-zone untrust policy zone-pol1]
```

```
  'match'
 VRF match criteria addition to VRF based zone is invalid
error: configuration check-out failed
[edit]
```

- Configuring more than 32 VRF instances in a zone results in a commit error as shown below:

```
user@host# commit
[edit security zones security-zone vrf-zone1 vrf]
 'VRF-c6'
 Exceeded the max number of vrfs (32)
error: configuration check-out failed
[edit]
```

- Associating the same VRF instance to multiple zones results in a commit error as shown below:

```
user@host#  commit
[edit security zones]
 'security-zone vrf-zone1'
   vrf VRF-a cannot be configured to multiple zones
error: configuration check-out failed
[edit]
```

- Configuring the same VRF instance in the VRF zone and the VRF group results in a commit error as shown below:

```
#
set security zones security-zone VRF2_ZONE vrf VRF1
set security zones security-zone VRF1_ZONE vrf VRF1
[edit]
user@host# set security l3vpn vrf-group G1 vrf VRF1

[edit]
root@10.205.54.84# commit check
[edit security l3vpn vrf-group G1 vrf]
  'VRF1'
    same vrf should not be in vrf-group and vrf-zone
error: configuration check-out failed: (statements constraint check failed)
```

Example: Configure Security Policies with VRF-Aware Security Zones to Manage VRF-Based Traffic

IN THIS SECTION

This example shows how to configure security policies with VRF-aware security zones to manage VRF-based traffic.

Requirements

- Understand how to create a security zone. See Example: Creating Security Zones.
- Supported SRX Series Firewall with any supported Junos OS release.
- Configure network interfaces on the device. See Interfaces User Guide for Security Devices.

Overview

In Junos OS, security policies enforce rules for transit traffic, in terms of what traffic can pass through the device and the actions that need to take place on the traffic as it passes through the device. An SRX Series Firewall is deployed in an SD-WAN to control traffic using the VRF-aware zone based security policies.

You can configure VRF-aware zone-based security policies with VRF instances, security zones, and inter-zone communication.

In this configuration example, you create two isolated virtual routing instances (VRF-a and VRF-b) that maintain separate routing and forwarding tables while enabling MPLS L3VPN functionality. Each VRF instance is associated with its own security zone, allowing granular security policy enforcement.

The configuration includes security policies that permit controlled communication between VRF instances and external networks through the trust zone. You can verify the configuration by checking VRF routing table isolation, security zone associations, and policy enforcement through traffic flow testing and monitoring commands.

Configuration

IN THIS SECTION

Configure VRF-aware zone-based security policies with VRF instances, security zones, and inter-zone communication to permit traffic.

Procedure

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

CLI Quick Configuration

```
set routing-instances VRF-a instance-type vrf
set routing-instances VRF-a route-distinguisher 10:200
set routing-instances VRF-a vrf-target target:100:100
set routing-instances VRF-a vrf-table-label
set routing-instances VRF-b instance-type vrf
set routing-instances VRF-b route-distinguisher 20:200
set routing-instances VRF-b vrf-target target:200:100
set routing-instances VRF-b vrf-table-label
set security zones security-zone vrf-zone1 vrf VRF-a
set security zones security-zone vrf-zone2 vrf VRF-b
set security policies from-zone vrf-zone1 to-zone vrf-zone2 policy pol1 match source-address any
set security policies from-zone vrf-zone1 to-zone vrf-zone2 policy pol1 match destination-
address any
set security policies from-zone vrf-zone1 to-zone vrf-zone2 policy pol1 match application any
set security policies from-zone vrf-zone1 to-zone vrf-zone2 policy pol1 match dynamic-
application any
set security policies from-zone vrf-zone1 to-zone vrf-zone2 policy pol1 then permit
set security zones security-zone trust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet address 4.0.0.254/8
set security policies from-zone vrf-zone1 to-zone trust policy pol2 match source-address any
set security policies from-zone vrf-zone1 to-zone trust policy pol2 match destination-address any
```

```
set security policies from-zone vrf-zone1 to-zone trust policy pol2 match application any
set security policies from-zone vrf-zone1 to-zone trust policy pol2 match dynamic-application any
set security policies from-zone vrf-zone1 to-zone trust policy pol2 then permit
```

Step-by-Step Procedure

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

1. Configure the VRF-a and VRF-b instances.

```
[edit routing-instances]
user@host# set VRF-a instance-type vrf
user@host# set VRF-b instance-type vrf
```

2. Assign a route distinguisher to each VRF routing instance.

```
[edit routing-instances]
user@host#set VRF-a route-distinguisher 10:200
user@host#set VRF-b route-distinguisher 20:200
```

3. Set a VRF target for each VRF routing instance.

```
[edit routing-instances]
user@host#set VRF-a vrf-target target:100:100
user@host#set VRF-b vrf-target target:200:100
```

   Setting different VRF targets ensures controlled route sharing between the VRF instances.

4. Assign a single VPN label for all the routes in the VRF instances.

```
[edit routing-instances]
user@host#set VRF-a vrf-table-label
user@host#set VRF-b vrf-table-label
```

5. Associate security zones to their respective defined VRF instances.

```
[edit security]
user@host#set security zones security-zone vrf-zone1 vrf VRF-a
user@host#set security zones security-zone vrf-zone2 vrf VRF-b
```

6. Configure the trust zone interface.

```
[edit security]
user@host#set security zones security-zone trust interfaces ge-0/0/0.0

user@host#set interfaces ge-0/0/0 unit 0 family inet address 4.0.0.254/8
```

Assign the management or shared services interface to the trust zone. This interface operates in the global routing table context. It provides access to shared services or management networks outside the VRF instance.

7. Configure an inter-VRF communication policy.

```
[edit security policies from-zone vrf-zone1 to-zone vrf-zone2]
user@host#set policy pol1 match source-address any
user@host#set policy pol1 match destination-address any
user@host#set policy pol1 match application any
user@host#set policy pol1 match dynamic-application any
user@host#set policy pol1 then permit
```

The policy `pol1` allows traffic from `vrf-zone1` to `vrf-zone2`. If `pol1` matches any source address, destination address, or applications, the `then permit` action allows the matched traffic to flow between VRF instances. This configuration creates a controlled bridge between otherwise isolated VRF instances.

8. Configure a policy to enable communication between VRF-a and the trust zone.

```
[edit security policies from-zone vrf-zone1 to-zone trust]
user@host#set policy pol2 match destination-address any
user@host#set policy pol2 match application any
```

```
user@host#set policy pol2 match dynamic-application any
user@host#set policy pol2 then permit
```

Policy `pol2` enables communication from vrf-zone1 to the trust zone. The policy also allows the VRF-a traffic to reach shared services in the global routing table and maintains broad matching criteria for maximum connectivity flexibility.

Results

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

```
[edit]
user@host#show security policies
from-zone vrf-zone1 to-zone vrf-zone2 {
    policy pol1 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application any;
        }
        then {
            permit;
        }
    }
}
from-zone vrf-zone1 to-zone trust {
    policy pol2 {
        match {
            source-address any;
            destination-address any;
            application any;
            dynamic-application any;
        }
        then {
            permit;
```

```
        }
    }
```

```
[edit]
user@host# show routing-instances
    VRF-a {
    instance-type vrf;
    route-distinguisher 10:200;
    vrf-target target:100:100;
    vrf-table-label;
}
VRF-b {
    instance-type vrf;
    route-distinguisher 20:200;
    vrf-target target:200:100;
    vrf-table-label;
}
```

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

Verification

IN THIS SECTION

Verify Policy Configuration

Purpose

Verify information about the configured security policies.

Action

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

```
user@root> show security policies
Default policy: deny-all
Default policy log Profile ID: 0
Pre ID default policy: permit-all
Default HTTP Mux policy: permit-all
From zone: vrf-zone1, To zone: vrf-zone2
  Policy: pol1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: any
    Source identity feeds: any
    Destination identity feeds: any
    Gbp source tags: 0
    Gbp destination tags: 0
    Action: permit
From zone: vrf-zone1, To zone: trust
  Policy: pol2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: any
    Source identity feeds: any
    Destination identity feeds: any
    Gbp source tags: 0
    Gbp destination tags: 0
    Action: permit
```

Verify Zone Configuration

Purpose

Verify information about the configured security zones.

Action

From operational mode, enter the `show security zones` command to display a summary of all the security zones configured on the device.

```
user@root> show security zones
Security zone: vrf-zone1
  Zone ID: 7
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
  Vrfs bound: 1
  Vrf:
    VRF-a
  Advanced-connection-tracking timeout: 1800
  Unidirectional-session-refreshing: No

Security zone: vrf-zone2
  Zone ID: 8
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
  Vrfs bound: 1
  Vrf:
    VRF-b
  Advanced-connection-tracking timeout: 1800
  Unidirectional-session-refreshing: No


Security zone: trust
  Zone ID: 9
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
```

```
Interfaces bound: 1
Interfaces:
  ge-0/0/1.0
Vrfs bound: 0
Vrf:
Advanced-connection-tracking timeout: 1800
Unidirectional-session-refreshing: No
```

RELATED DOCUMENTATION

Flow Management in SRX Series Devices Using VRF Routing Instance

Understanding ALG Support for VRF Routing Instance

NAT for VRF Routing Instance

9

CHAPTER

Monitor Security Policies

IN THIS CHAPTER

Monitoring and Troubleshooting Security Policies

IN THIS SECTION

Monitoring provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and effect operational conditions. Troubleshooting provides contextual guidance for resolving the access issues on networks. You can then address user concerns and provide resolution in a timely manner.

Understanding Security Alarms

Alarms are triggered when packets are dropped because of a policy violation. A policy violation occurs when a packet matches a reject or deny policy. A policy violation alarm is generated when the system monitors any of the following audited events:

- Number of policy violations by a source network identifier within a specified period
- Number of policy violations to a destination network identifier within a specified period
- Number of policy violations to an application within a specified period
- Policy rule or group of rule violations within a specified period

There are four types of alarms corresponding to these four events. The alarms are based on source IP, destination IP, application, and policy.

When a packet encounters a reject or deny policy, the policy violation counters for all enabled types of alarm are increased. When any counter reaches the specified threshold within a specified period, an alarm is generated. After a specified period, the policy violation counter is reset and reused to start another counting cycle.

To view the alarm information, run the `show security alarms` command. The violation count and the alarm do not persist across system reboots. After a reboot, the violation count resets to zero and the alarm is cleared from the alarm queue.

After taking appropriate actions, you can clear the alarm. The alarm remains in the queue until you clear it (or until you reboot the device). To clear the alarm, run the `clear security alarms` command. After you clear the alarm, a subsequent series of flow policy violations can cause a new alarm to be raised.

SEE ALSO

Example: Setting an Audible Alert as Notification of a Security Alarm

Example: Generating a Security Alarm in Response to Policy Violations

IN THIS SECTION

This example shows how to configure the device to generate a system alarm when a policy violation occurs. By default, no alarm is raised when a policy violation occurs.

Requirements

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

Overview

In this example, you configure an alarm to be raised when:

- The application size is 10240 units.
- The source IP violation exceeds 1000 within 20 seconds.
- The destination IP violations exceeds 1000 within 10 seconds.
- The policy match violation exceeds 100, with a size of 100 units.

Configuration

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 alarms potential-violation policy application size 10240
set security alarms potential-violation policy source-ip threshold 1000 duration 20
set security alarms potential-violation policy destination-ip threshold 1000 duration 10
set security alarms potential-violation policy policy-match threshold 100 size 100
```

Step-by-Step Procedure

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

To configure policy violation alarms:

1. Enable security alarms.

```
[edit]
user@host# edit security alarms
```

2. Specify that an alarm should be raised when an application violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set application size 10240
```

3. Specify that an alarm should be raised when a source IP violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set source-ip threshold 1000 duration 20
```

4. Specify that an alarm should be raised when a destination IP violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set destination-ip threshold 1000 duration 10
```

5. Specify that an alarm should be raised when a policy match violation occurs.

```
[edit security alarms potential-violation policy]
user@host# set policy-match threshold 100 size 100
```

Results

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

```
policy {
    source-ip {
        threshold 1000;
        duration 20;
    }
    destination-ip {
```

```
        threshold 1000;
        duration 10;
    }
    application {
        size 10240;
    }
    policy-match {
        threshold 100;
        size 100;
    }
}
```

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

Verification

To confirm that the configuration is working properly, from operational mode, enter the `show security alarms` command.

Matching Security Policies

The `show security match-policies` command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, the `show security match-policies` command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The `result-count` option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are “shadowed” by the first and are never encountered by matching traffic.

> **NOTE**: The `show security match-policies` command is applicable only to security policies; IDP policies are not supported.

Example 1: show security match-policies

```
user@host> show security match-policies from-zone z1 to-zone z2  source-ip 10.10.10.1
destination-ip 192.0.2.1 source-port 1 destination-port 21 protocol tcp
Policy: p1, action-type: permit, State: enabled, Index: 4
```

```
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 203.0.113.1/25
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 203.0.113.129/25
    d3: 192.0.2.1/24
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
    Source port range: [0-0]
    Destination port range: [21-21]
```

Example 2: Using the result-count Option

By default, the output list contains the policy that will be applied to traffic with the specified characteristics. To list more than one policy that match the criteria, use the `result-count` option. The first policy listed is always the policy that will be applied to matching traffic. If the `result-count` value is from 2 to 16, the output includes all policies that match the criteria up to the specified `result-count`. All policies listed after the first are “shadowed” by the first policy and are never applied to matching traffic.

Use this option to test the positioning of a new policy or to troubleshoot a policy that is not applied as expected for particular traffic.

In the following example, the traffic criteria matches two policies. The first policy listed, `p1`, contains the action applied to the traffic. Policy `p15` is shadowed by the first policy, and its action, therefore, will not be applied to matching traffic.

```
user@host> show security match-policies from-zone zone-A to-zone zone-B source-ip 10.10.10.1
destination-ip 192.0.2.1 source-port 1004 destination-port 80 protocol tcp result-count 5
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 192.0.2.0/24
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
    Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
```

```
Sequence number: 15
From zone: zone-A, To zone: zone-B
Source addresses:
  sa11: 10.10.10.1/32
Destination addresses:
  da15: 192.0.2.5/24
Application: any
  IP protocol: 1, ALG: 0, Inactivity timeout: 0
  Source port range: [1000-1030]
  Destination port range: [80-80]
```

SEE ALSO

Understanding Security Policy Rules | 97
Understanding Security Policy Elements | 96

Tracking Policy Hit Counts

Use the `show security policies hit-count` command to display the utility rate of security policies according to the number of hits they receive. You can use this feature to determine which policies are being used on the device, and how frequently they are used. Depending on the command options that you choose, the number of hits can be listed without an order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

Checking Memory Usage

You can isolate memory issues by comparing memory values before and after policy configurations.

Certain practices can help monitor the current memory usage on the device and optimize parameters to better size system configuration, especially during policy implementation.

To check memory usage:

- Use the `show chassis routing-engine` command to check overall Routing Engine (RE) memory usage. The following output from this command shows memory utilization at 39 percent:

```
user@host# show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    DRAM                      1024 MB
    Memory utilization          39 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     2 percent
      Interrupt                  0 percent
      Idle                      97 percent
    Model                          RE-PPC-1200-A
    Start time                     2011-07-09 19:19:49 PDT
    Uptime                         37 days, 15 hours, 44 minutes, 13 seconds
    Last reboot reason             0x3:power cycle/failure watchdog
    Load averages:                 1 minute   5 minute  15 minute
                                       0.22       0.16       0.07
```

- Use the `show system processes extensive` command to acquire information on the processes running on the Routing Engine.

  Use the `find nsd` option in the `show system processes extensive` command to see direct usage on the Network Security Daemon (NSD) with its total memory in use as 10 megabytes and CPU utilization of 0 percent.

```
user@host# show system processes extensive | find nsd
 1182 root         1  96    0 10976K  5676K select   2:08  0.00% nsd
 1191 root         4   4    0  8724K  3764K select   1:57  0.00% slbd
 1169 root         1  96    0  8096K  3520K select   1:51  0.00% jsrpd
 1200 root         1   4    0     0K    16K peer_s   1:10  0.00% peer proxy
 1144 root         1  96    0  9616K  3528K select   1:08  0.00% lacpd
 1138 root         1  96    0  6488K  2932K select   1:02  0.00% ppmd
 1130 root         1  96    0  7204K  2208K select   1:02  0.00% craftd
 1163 root         1  96    0 16928K  5188K select   0:58  0.00% cosd
 1196 root         1   4    0     0K    16K peer_s   0:54  0.00% peer proxy
```

```
   47 root          1 -16    0     0K    16K sdflus   0:54  0.00% softdepflush
 1151 root          1  96    0 15516K  9580K select   0:53  0.00% appidd
  900 root          1  96    0  5984K  2876K select   0:41  0.00% eventd
```

- Check the configuration file size. Save your configuration file with a unique name before exiting the CLI. Then, enter the `ls -l filename` command from the shell prompt in the UNIX-level shell to check the file size as shown in the following sample output:

```
user@host> start shell
% ls -l config
-rw-r--r--  1 remote  staff  12681 Feb 15 00:43 config
```

SEE ALSO

Best Practices for Defining Policies | 105
Security Policies Overview | 2

Monitor Security Policy Statistics

IN THIS SECTION

Purpose

Monitor and record traffic that Junos OS permits or denies based on previously configured policies.

Action

To monitor traffic, enable the count and log options.

Count—Configurable in an individual policy. If count is enabled, statistics are collected for sessions that enter the device for a given policy, and for the number of packets and bytes that pass through the device in both directions for a given policy. For counts (only for packets and bytes), you can specify that alarms be generated whenever the traffic exceeds specified thresholds. See count (Security Policies).

Log—Logging capability can be enabled with security policies during session initialization (**session-init**) or session close (**session-close**) stage. See log (Security Policies).

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

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

For details about information collected for session logs, see Information Provided in Session Log Entries for SRX Series Services Gateways.

Verifying Shadow Policies

IN THIS SECTION

Verifying All Shadow Policies

IN THIS SECTION

Purpose

Verify all the policies that shadows one or more policies.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the `show security shadow-policies logical-system` *`lsys-name`* `from-zone` *`from-zone-name`* `to-zone` *`to-zone-name`* command.
- For global policies, enter the `show security shadow-policies logical-system` *`lsys-name`* `global` command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b
    Policies               Shadowed policies
    P1                     P3
    P1                     P4
    P2                     P5
```

Meaning

The output displays the list of all policies that shadows other policies. In this example, P1 policy shadows P3 and P4 policies and P2 policy shadows P5 policy.

Verifying a Policy Shadows One or More Policies

IN THIS SECTION

Purpose

Verify if a given policy shadows one or more policies positioned after it.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the `show security shadow-policies logical-system` *`lsys-name`* `from-zone` *`from-zone-name`* `to-zone` *`to-zone-name`* `policy` *`policy-name`* command.
- For global policies, enter the `show security shadow-policies logical-system` *`lsys-name`* `global policy` *`policy-name`* command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P1
   Policies                   Shadowed policies
    P1                          P3
    P1                          P4
```

Meaning

The output displays all the policies that are shadowed by the given policy. In this example, P1 policy shadows P3 and P4 policies.

Verifying a Policy Is Shadowed by One or More Policies

IN THIS SECTION

Purpose

Verify if a given policy is shadowed by one or more positioned before it.

Action

From the operational mode, enter the following commands:

- For logical systems, enter the `show security shadow-policies logical-system` *`lsys-name`* `from-zone` *`from-zone-name`* `to-zone` *`to-zone-name`* `policy` *`policy-name`* `reverse` command.

- For global policies, enter the `show security shadow-policies logical-system *lsys-name* global policy *policy-name* reverse` command.

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse
   Policies                Shadowed policies
    P1                      P4
```

Meaning

The output displays the given policy shadowed by one or more policies. In this example, P4 policy is shadowed by P1 policy.

RELATED DOCUMENTATION

View and Change Security Policy Ordering | 223

Example: Reordering Security Policies

Troubleshoot Security Policies

IN THIS SECTION

Synchronize Policies Between Routing Engine and Packet Forwarding Engine

IN THIS SECTION

Problem

Description

Security policies are stored in the routing engine and the packet forwarding engine. Security policies are pushed from the Routing Engine to the Packet Forwarding Engine when you commit configurations. If the security policies on the Routing Engine are out of sync with the Packet Forwarding Engine, the commit of a configuration fails. Core dump files may be generated if the commit is tried repeatedly. The out of sync can be due to:

- A policy message from Routing Engine to the Packet Forwarding Engine is lost in transit.
- An error with the routing engine, such as a reused policy UID.

Environment

The policies in the Routing Engine and Packet Forwarding Engine must be in sync for the configuration to be committed. However, under certain circumstances, policies in the Routing Engine and the Packet Forwarding Engine might be out of sync, which causes the commit to fail.

Symptoms

When the policy configurations are modified and the policies are out of sync, the following error message displays - `error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)> Please request security policies check/resync.`

Solution

Use the `show security policies checksum` command to display the security policy checksum value and use the `request security policies resync` command to synchronize the configuration of security policies in the Routing Engine and Packet Forwarding Engine, if the security policies are out of sync.

Check a Security Policy Commit Failure

IN THIS SECTION

Problem

Description

Most policy configuration failures occur during a commit or runtime.

Commit failures are reported directly on the CLI when you execute the CLI command **commit-check** in configuration mode. These errors are configuration errors, and you cannot commit the configuration without fixing these errors.

Solution

To fix these errors, do the following:

1. Review your configuration data.
2. Open the file /var/log/nsd_chk_only. This file is overwritten each time you perform a commit check and contains detailed failure information.

Verify a Security Policy Commit

IN THIS SECTION

Problem

Description

Upon performing a policy configuration commit, if you notice that the system behavior is incorrect, use the following steps to troubleshoot this problem:

Solution

1. Operational **show** Commands—Execute the operational commands for security policies and verify that the information shown in the output is consistent with what you expected. If not, the configuration needs to be changed appropriately.

2. Traceoptions—Set the `traceoptions` command in your policy configuration. The flags under this hierarchy can be selected as per user analysis of the `show` command output. If you cannot determine what flag to use, the flag option `all` can be used to capture all trace logs.

   ```
   user@host# set security policies traceoptions <flag all>
   ```

You can also configure an optional filename to capture the logs.

```
user@host# set security policies traceoptions <filename>
```

If you specified a filename in the trace options, you can look in the /var/log/<*filename*> for the log file to ascertain if any errors were reported in the file. (If you did not specify a filename, the default filename is eventd.) The error messages indicate the place of failure and the appropriate reason.

After configuring the trace options, you must recommit the configuration change that caused the incorrect system behavior.

Debug Policy Lookup

IN THIS SECTION

Problem

Description

When you have the correct configuration, but some traffic was incorrectly dropped or permitted, you can enable the `lookup` flag in the security policies traceoptions. The `lookup` flag logs the lookup related traces in the trace file.

Solution

```
user@host# set security policies traceoptions <flag lookup>
```

High Availability (HA) Synchronization of Address Name Resolving Cache

The Network security process (NSD) restarts when system reboots, HA failover happens, or if the process crashes. During this time, if there are large number of domain name addresses configured in the security polices, SRX Firewalls attempt to send requests to DNS server to get all resolved IP addresses. A high amount of system resources are consumed when a large number of DNS queries and responses are exchanged. So, SRX Firewalls are unable to obtain a response from the DNS server and the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found. The new enhancement on SRX Firewalls addresses this problem by caching the DNS query results into a local DNS cache file and periodically synchronizing the DNS cache file from HA primary node to HA backup node. The DNS cache files stores IP addresses, domain name, and TTL values. After the HA failover, the previous backup node becomes primary node. Since all DNS cache results are available on new primary node, security policy processing continues and pass-through traffic is allowed as per the policy rules.

Starting in Junos OS Release 19.3R1, the policy DNS cache memory is synchronized into one local DNS cache file on the HA active node and is copied to the HA backup node to suppress DNS queries or responses during NSD restart.

The following steps are performed for the synchronization to take place:

1. The policy DNS cache memory is synchronized into one local policy DNS cache file located at the */var/db/policy_dns_cache* path every 30 seconds if the policy DNS cache memory content has changed during this period.

2. The local DNS cache file is synchronized from the HA primary node to HA backup node immediately after the local DNS cache file has been updated in Step 1.

The synchronization includes the following content:

- Domain name
- IPv4 address list and its TTL (time to live)
- IPv6 address list and its TTL

When NSD restarts, it reads and parses the local DNS cache file and imports all cache entries into memory. The synchronization ensures that DNS queries are suppressed during an NSD restart. NSD restarts on new primary node during HA failover as the resolved IP addresses for domain names already exist in DNS cache memory when reading policies configurations. Therefore, new pass-through traffic is allowed as per the security policy after HA failover because all resolved IP addresses for domain names exist inside policies on new primary node's Routing Engine and Packet Forwarding Engine.

Platform-Specific Memory Usage Behavior

Use Feature Explorer to confirm platform and release support for specific features.

Use the following table to review platform-specific behavior for your platform:

Platform	Difference
SRX Series	• On SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices, that support High Availability (HA) synchronization of address names, the memory for flow entities such as policies, zones, or addresses is dynamically allocated (depending on the Junos OS release in your installation).

RELATED DOCUMENTATION

Security Policies Overview | 2