JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Common Criteria Guide for SRX345, SRX345-DUAL-AC, and SRX380 in Cluster Mode

Published
2021-10-01

RELEASE
20.4R1

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

Junos® OS Common Criteria Guide for SRX345, SRX345-DUAL-AC, and SRX380 in Cluster Mode
20.4R1

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 and evaluate SRX Series devices for Common Criteria (CC) compliance. Common Criteria for information technology is an international agreement signed by several countries that permit the evaluation of security products against a common set of standards.

RELATED DOCUMENTATION

- Common Criteria and FIPS Certifications

1
CHAPTER

Overview

Understanding the Common Criteria Evaluated Configuration

IN THIS SECTION

This document describes the steps required to duplicate the configuration of the device running Junos OS when the device is evaluated. This is referred to as the evaluated configuration.

These documents are available at https://www.niap-ccevs.org/Profile/PP.cfm?archived=1.

NOTE: On SRX345 and SRX380 devices, Junos OS Release 20.4R1 is certified for Common Criteria with FIPS mode enabled on the devices.

Understanding Common Criteria

Common Criteria for information technology is an international agreement signed by several countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at http://www.commoncriteriaportal.org/ccra/, the participants agree to mutually recognize evaluations of products performed in other countries. All evaluations are performed using a common methodology for information technology security evaluation.

For more information on Common Criteria, see http://www.commoncriteriaportal.org/.

Supported Platforms

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

- SRX345 devices.

- SRX345-DUAL-AC devices.
- SRX380 devices.

RELATED DOCUMENTATION

> *Identifying Secure Product Delivery*

Identifying Secure Product Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform.

- Shipping label—Ensure that the shipping label correctly identifies the correct customer name and address as well as the device.
- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.
- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.
- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:
    - Purchase order number

- Juniper Networks order number used to track the shipment
- Carrier tracking number used to track the shipment
- List of items shipped including serial numbers
- Address and contacts of both the supplier and the customer

- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, you should perform the following tasks:
  - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.
  - Log on to the Juniper Networks online customer support portal at https://support.juniper.net/support to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

RELATED DOCUMENTATION

Understanding the Common Criteria Evaluated Configuration | 2

Understanding Management Interfaces

The following management interfaces can be used in the evaluated configuration:

- Local Management Interfaces—The RJ-45 console port on the rear panel of a device is configured as RS-232 data terminal equipment (DTE). You can use the command-line interface (CLI) over this port to configure the device from a terminal.
- Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration, and it is enabled by default on the device. The remote management protocols J-Web and Telnet are not available for use on the device in the evaluated configuration.

CHAPTER 2

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in the CC Evaluated Configuration

IN THIS SECTION

Administrator Role and Responsibilities

The Administrator is the person responsible for operating Junos OS in the Evaluated Configuration. The Administrator also securely installs Junos OS on the device, enables FIPS mode of operation, establishes keys and passwords for other users and software modules, and initializes the device before network connection. The Administrator can configure and monitor the module through a console or SSH connection.

User Roles and Responsibilities

The user assigned with the Administrator role, can view or modify the configuration. No other users or classes are considered in the Evaluated Configuration.

What Is Expected of All Users

All FIPS users, including the Security Administrator, must observe security guidelines at all times. An Administrator user must observe security guidelines at all times. They must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.

- Check audit files periodically.
- Follow these guidelines:
  - All users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

Downloading Software Packages from Juniper Networks

To operate in Junos OS in the Evaluated Configuration, the device must have the following software packages installed. You can download them from the Juniper Networks website:

- Junos OS for SRX345 and SRX380 devices, Release 20.4R1

Before you begin to download the software, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: https://userregistration.juniper.net/entitlement/setupAccountInfo.do.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. https://support.juniper.net/support/downloads/
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Download the software. See Downloading Software.

RELATED DOCUMENTATION

Installation and Upgrade Guide

Installing Junos Software Packages

The evaluated configuration requires the SRX345 and SRX380 to operate in FIPS mode.

> **NOTE**: Junos OS is delivered in signed packages that contain digital signatures to ensure the Juniper Networks software is running. When installing the software packages, Junos OS validates the signatures and the public key certificates used to digitally sign the software packages. If the signature or certificate is found to be invalid (for example, when the certificate validity period has expired or cannot be verified against the root CA stored in the Junos OS internal store), the installation process fails.

To install these software packages, perform the following tasks:

1. Download the Junos OS package from https://support.juniper.net/support/downloads/. See Downloading Software.
2. Install Junos OS on your device using the following CLI command: `request system software add /<image-path>/<junos package> no-copy no-validate reboot`.

RELATED DOCUMENTATION

- Installation and Upgrade Guide

Understanding Zeroization

IN THIS SECTION

Zeroization completely erases all configuration information on the device, including all plaintext passwords, secrets, and private keys for SSH, local encryption, local authentication, and IPsec. To exit the evaluated configuration, you need to zeroize the device.

For SRX345, SRX345-DUAL-AC and SRX380 devices, the Administrator initiates the zeroization process by entering `request system zeroize` from the CLI.

The cryptographic module provides a non-approved mode of operation in which non-approved cryptographic algorithms are supported. When moving from the non-approved mode of operation to the approved mode of operation, the Cryptographic Officer must zeroize the non-approved mode critical security parameters (CSPs). For SRX345 and SRX380 devices, the Cryptographic Officer initiates the zeroization process by entering the `request system zeroize` from the CLI after enabling FIPS mode of operation. Use of this command is restricted to the Cryptographic Officer.

CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the device.

When to Zeroize?

As an Administrator, perform zeroization in the following situations:

- **Before entering the evaluated configuration**—To prepare your device for the evaluated mode of operation as a FIPS cryptographic module, perform zeroization to remove any non-approved configuration and enable the FIPS mode on the device.
- • **To remove the evaluated configuration**—To remove the evaluated configuration and to begin repurposing your device for non-FIPS operation, perform zeroization on the device.

How to Enable and Configure FIPS Mode in Junos OS

To enable the FIPS mode in Junos OS, perform the following steps:

1. Zeroize the device before enabling FIPS mode of operation

   `user@host>` **request system zerioze**

2. Enable the FIPS mode on the device.

   `user@host#` **set system fips level 2**

3. Set the root password.

```
user@host# set system root-authentication plain-text-password

New password: type password here

Retype new password: retype password here
```

4. Remove the CSPs on commit check and reboot the device.

```
user@host# commit
```

5. After you reboot the device, perform integrity and self-tests when the module is operating in FIPS mode.

```
user@host:fips> show version
Hostname: host-srx380
Model: srx380-poe-ac
Junos: 20.4R1
JUNOS Software Release [20.2R1]
```

RELATED DOCUMENTATION

Loading Firmware on the Device

3
CHAPTER

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Administrator

The Administrator role is associated with a defined login class, and the administrator is assigned with all permissions. Data is stored locally for fixed password authentication.

NOTE: We recommend that you not use control characters in passwords.

Use the following guidelines and configuration options for passwords and when selecting passwords for authorized administrator accounts. Passwords should be:

- Easy to remember so that users are not tempted to write it down.
- Changed periodically.
- Private and not shared with anyone.
- Contain a minimum of 10 characters. The minimum password length is 10 characters.

```
[ edit ]
administrator@host# set system login password minimum-length 10
```

- Include both alphanumeric and punctuation characters, composed of any combination of upper and lowercase letters, numbers, and special characters such as, “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. There should be at least a change in one case, one or more digits, and one or more punctuation marks.
- Contain character sets. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.

```
[ edit ]
administrator@host# set system login password change-type character-sets
```

- Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos is 2.

```
[ edit ]
administrator@host# set system login password minimum-changes 2
```

NOTE: The authentication algorithm for plain-text passwords must be configured as sha256.

```
[ edit ]
administrator@host# set system login password format sha256
```

When you change the password algorithm to SHA256, change even the user password. Until then, the old hash algorithm is used.

Weak passwords are:

- Words that might be found in or exist as a permuted form in a system file such as **/etc/passwd**.
- The hostname of the system (always a first guess).
- Any words appearing in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, and television shows.
- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (for example f00t) or with digits added to the end.
- Any machine-generated passwords. Algorithms reduce the search space of password-guessing programs and so should not be used.

Strong reusable passwords can be based on letters from a favorite phrase or word, and then concatenated with other, unrelated words, along with additional digits and punctuation.

NOTE: Passwords should be changed periodically.

RELATED DOCUMENTATION

Identifying Secure Product Delivery | 3

Configuring an Authorized Administrator for the Evaluated Configuration

An account for `root` is always present in a configuration and is not intended for use in normal operation. In the evaluated configuration, the `root` account is restricted to the initial installation and configuration of the evaluated device.

The authorized administrator must have all permissions, including the ability to change the router configuration.

To configure an authorized administrator:

1. Create a login class named security-admin with all permissions.

```
[edit]
root@host# set system login class security-admin permissions all
```

2. Define your user as an authorized administrator.

```
[edit]
root@host# set system login user EC-user class security-admin authentication encrypted-
password
```

OR

```
[edit]
root@host# set system login user EC-user class security-admin authentication plain-text-
password
```

3. Configure the authentication algorithm for plain-text passwords as sha256.

```
[edit]
root@host# set system login password format sha256
```

4. Commit the changes.

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

NOTE: The root password should be reset following the change to sha256 for the password storage format. This ensures the new password is protected using a sha256 hash, rather than the default password hashing algorithm. To reset the root password, use the `set system login user root password` *password* command, and confirm the new password when prompted.

RELATED DOCUMENTATION

Understanding the Associated Password Rules for an Administrator | 12

4

CHAPTER

Configuring SSH and Console Connection

Understanding Authentication Methods

IN THIS SECTION

The Juniper Networks Junos operating system (Junos OS) running in evaluated configuration mode of operation allows a wide range of capabilities for users, and authentication is role-based. The following types of role-based authentication are supported in the evaluated configuration mode of operation:

- "Username and Password Authentication over the Console and SSH" on page 17
- "Username and Public Key Authentication over SSH" on page 18

Username and Password Authentication over the Console and SSH

In this authentication method, the user is requested to enter the username and password. The device enforces the user to enter a minimum of 10 characters password that is chosen from the 96 human-readable ASCII characters.

NOTE: The maximum password length is 20 characters.

In this method, the device enforces a timed access mechanism—for example, first two failed attempts to enter the correct password (assuming 0 time to process), no timed access is enforced. When the user enters the password for the third time, the module enforces a 5 second delay. Each failed attempt thereafter results in an additional 5 second delay above the previous failed attempt. For example, if the fourth failed attempt is a 10 second delay, then the fifth failed attempt is a 15 second delay, the sixth failed attempt is a 20 second delay, and the seventh failed attempt is a 25 second delay.

Therefore, this leads to a maximum of seven possible attempts in a 1 minute period for each getty active terminal. So, the best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour or 60 minutes). This would be rounded off to 9 attempts per minute, because there is no such thing as 0.6 attempts. Thus the probability of a successful random attempt is

1/9610, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a 1 minute period is 9/(9610), which is less than 1/100,000.

Username and Public Key Authentication over SSH

In SSH public key authentication, you provide the username and validate the ownership of the private key corresponding to the public key stored on the server. The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048, 3072, and 4092 modulus bit length) key-types. The probability of a success with multiple consecutive attempts in a 1-minute period is 5.6e7/(2128).

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration | 21

Configuring a System Login Message and Announcement

A system login message appears before the user logs in and a system login announcement appears after the user logs in. By default, no login message or announcement is displayed on the device.

To configure a system login message, use the following command:

```
[edit]
user@host# set system login message login-message-banner-text
```

To configure system announcement, use the following command:

```
[edit]
user@host# set system login announcement  system-announcement-text
```

NOTE:

- If the message text contains any spaces, enclose it in quotation marks.
- You can format the message using the following special characters:
  - \n—New line
  - \t—Horizontal tab
  - \'—Single quotation mark
  - \"—Double quotation mark
  - \\—Backslash

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration | 21

Limiting the Number of User Login Attempts for SSH Sessions

A remote administrator may login to a device through SSH. Administrator credentials are stored locally on the device. If the remote administrator presents a valid username and password, access to the TOE is granted. If the credentials are invalid, the TOE allows the authentication to be retried after an interval that starts after 1 second and increases exponentially. If the number of authentication attempts exceed the configured maximum, no authentication attempts are accepted for a configured time interval. When the interval expires, authentication attempts are again accepted.

You can configure the device to limit the number of attempts to enter a password while logging through SSH. Using the following command, the connection can be terminated if a user fails to login after a specified number of attempts:

The number of reattempts the device allows is defined by the `tries-before-disconnect` option. The device allows 10 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator

manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console

```
[edit system login]
user@host# set retry-options tries-before-disconnect <number>
```

Here, `tries-before-disconnect` is the number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default value is 10.

You can also configure a delay, in seconds, before a user can try to enter a password after a failed attempt.

```
[edit system login]
user@host# set retry-options backoff-threshold  <number>
```

Here, `backoff-threshold` is the threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. The range is from 1 through 3, and the default value is 2 seconds. Use the `backoff-factor` option to specify the length of the delay in seconds.

In addition, the device can be configured to specify the threshold for the number of failed attempts before the user experiences a delay in entering the password again.

```
[edit system login]
user@host# set retry-options backoff-factor  <number>
```

Here, `backoff-factor` is the length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default value is 5 seconds.

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration | 21

Configuring SSH on the Evaluated Configuration

SSH is an allowed remote management interface in the evaluated configuration. This topic describes how to configure SSH on the device.

1. Before you begin, log in with your root account on the device running Junos OS Release 20.4R1 and edit the configuration.

NOTE: The commands shown configure SSH to use all of the allowed cryptographic algorithms.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure SSH on the TOE:

1. Specify the permissible SSH host-key algorithms.

```
[edit system services ssh]
user@host# set hostkey-algorithm ssh-ecdsa
user@host# set hostkey-algorithm ssh-rsa
```

2. Specify the SSH key-exchange algorithms.

```
[edit system services ssh]
user@host#set key-exchange [ ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 ]
```

3. Specify all the permissible message authentication code algorithms.

```
[edit system services ssh]
user@host#set macs [ hmac-sha2-256 hmac-sha2-512 ]
```

4. Specify the ciphers allowed for protocol version 2.

```
[edit system services ssh]
user@host#set ciphers [ aes128-cbc aes256-cbc aes128-ctr aes256-ctr ]
```

5
CHAPTER

Configuring the Remote Syslog Server

Sample Syslog Server Configuration on a Linux System

IN THIS SECTION

A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.

The logs capture the events, few of them are listed below:

- Committed changes
- Login and logout of users
- Failure to establish an SSH session
- Establishment or termination of an SSH session
- Changes to the system time

Configuring Event Logging to a Local File

You can configure storing of messages to a local file and the level of detail to be recorded with the `syslog` statement. This example stores logs in a file named **syslog**:

```
[edit system]
syslog {
    file syslog;
}
```

Configuring Event Logging to a Remote Server

Configure the export of audit information to a secure, remote server by setting up an event trace monitor that sends event log messages by using NETCONF over SSH to the remote system event logging server. The following procedures show the configuration needed to send system log messages to a secure external server by using NETCONF over SSH.

Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server

The following procedure describes the steps to configure event logging to a remote server when the SSH connection to the TOE is initiated from the remote system log server.

1. Generate an RSA public key on the remote syslog server.

```
$ ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
```

   You will be prompted to enter the desired passphrase. The storage location for the `syslog-monitor` key pair is displayed.

2. On the TOE, create a class named `monitor` that has permission to trace events.

```
[edit]
user@host# set system login class monitor permissions trace
```

3. Create a user named `syslog-mon` with the class monitor, and with authentication that uses the `syslog-monitor` key pair from the key pair file located on the remote syslog server.

```
[edit]
user@host# set system login user syslog-mon class monitor authentication ssh-rsa public key
from syslog-monitor key pair
```

4. Set up NETCONF with SSH.

```
[edit]
user@host# set system services netconf ssh
```

5. Configure syslog to log all the messages at */var/log/messages*.

```
[edit]
user@host# set system syslog file messages any any
user@host# commit
```

6. On the remote system log server, start up the SSH agent. The start up is required to simplify the handling of the syslog-monitor key.

```
$ eval `ssh-agent`
```

7. On the remote syslog server, add the `syslog-monitor` key pair to the SSH agent.

```
$ ssh-add ~/.ssh/syslog-monitor
```

You will be prompted to enter the desired passphrase. Enter the same passphrase used in Step 1.

8. After logging in to the `external_syslog_server` session, establish a tunnel to the device and start NETCONF.

```
user@host# ssh syslog-mon@TOE -s netconf > test.out
```

9. After NETCONF is established, configure a system log events message stream. This RPC will cause the NETCONF service to start transmitting messages over the SSH connection that is established.

```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```

10. The examples for syslog messages are listed below. Monitor the event log generated for admin actions on TOE as received on the syslog server. Examine the traffic that passes between the audit server and the TOE, observing that these data are not viewed during this transfer, and that they are successfully received by the audit server. Match the logs between local event and the remote event logged in a syslog server and record the particular software (such as name, version, and so on) used on the audit server during testing.

The following output shows test log results for syslog server.

```
host@ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /home/host/.ssh/syslog-monitor.
Your public key has been saved in /home/host/.ssh/syslog-monitor.pub.
The key fingerprint is:
ef:75:d7:68:c5:ad:8d:6f:5e:7a:7e:9b:3d:f1:4d:3f syslog-monitor key pair
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|               ..|
|        S       +|
|         .     Bo|
|          . . *.X|
|         . . o E@|
|          .   .BX|
+-----------------+
[host@linux]$ cat /home/host/.ssh/syslog-monitor.pub
ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAABAQCrUREJUBpjwAoIgRrGy9zgt+
D2pikk3Q/Wdf8I5vr+njeqJhCx2bUAkrRbYXNILQQAZbg7kLfi/8TqqL
eon4HOP2e6oCSorKdx/GrOTzLONL4fh0EyuSAk8bs5JuwWNBUokV025
gzpGFsBusGnlj6wqqJ/sjFsMmfxyCkbY+pUWb8m1/A9YjOFT+6esw+9S
tF6Gbg+VpbYYk/Oday4z+z7tQHRFSrxj2G92aoliVDBLJparEMBc8w
LdSUDxmgBTM2oadOmm+kreBUQjrmr6775RJn9H9YwIxKOxGm4SFnX/Vl4
R+lZ9RqmKH2wodIEM34K0wXEHzAzNZ01oLmaAVqT
syslog-monitor key pair
[host@linux]$ eval `ssh-agent `
Agent pid 1453
[host@linux]$ ssh-add ~/.ssh/syslog-monitor
Enter passphrase for /home/host/.ssh/syslog-monitor:
Identity added: /home/host/.ssh/syslog-monitor (/home/host/.ssh/syslog-monitor)
```

Net configuration channel

```
host@linux]$ ssh syslog-mon@starfire -s netconf>test.out
host@linux]$ cat test.out
this is NDcPP test device

<!-- No zombies were killed during the creation of this user interface --
<!-- user syslog-mon, class j-monitor -><hello>
  <capabilities>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
```

```
    <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</
capability>
    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
  </capabilities>
  <session-id4129/session-id>
</hello>
]]>]]>
```

The following output shows event logs generated on the TOE that are received on the syslog server.

```
Jan 20 17:04:51  starfire sshd[4182]: error: Could not load host key: /etc/ssh/ssh_host_dsa_key
Jan 20 17:04:51  starfire sshd[4182]: error: Could not load host key: /etc/ssh/ssh_host_ecdsa_key
Jan 20 17:04:53  starfire sshd[4182]: Accepted password for sec-admin from 10.209.11.24 port
55571 ssh2
Jan 20 17:04:53  starfire mgd[4186]: UI_AUTH_EVENT: Authenticated user 'sec-admin' at permission
level 'j-administrator'
Jan 20 17:04:53  starfire mgd[4186]: UI_LOGIN_EVENT: User 'sec-admin' login, class 'j-
administrator' [4186], ssh-connection '10.209.11.24 55571 10.209.14.92 22', client-mode 'cli'
```

Net configuration channel

```
host@linux]$ ssh syslog-mon@starfire -s netconf
 this is NDcPP test device

<!-- No zombies were killed during the creation of this user interface --
<!-- user syslog-mon, class j-monitor -><hello>
  <capabilities>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</
capability>
    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
  </capabilities>
```

```
  <session-id4129/session-id>
</hello>
]]>]]>
```

The following output shows that the local syslogs and remote syslogs received are similar.

```
Local : an 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Redundancy interface management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/rdd', PID 4317,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Dynamic
flow capture service checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/dfcd', PID 4318,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Connectivity fault management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/cfmd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/cfmd', PID 4319,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
address flooding and learning process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2ald'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2ald', PID 4320,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
Control Protocol process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2cpd'
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30  starfire l2cp[4321]: Initialized 802.1X module and state machinesJan 20
17:09:30  starfire l2cp[4321]: Read acess profile () config
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2cpd', PID 4321,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Multicast
Snooping process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/mcsnoopd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/mcsnoopd', PID
4325, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: commit
wrapup...
```

```
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
activating '/var/etc/ntp.conf'
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: start ffp
activate
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30  starfire ffp[4326]: "dynamic-profiles": No change to
profiles.....................................
```

```
Remote : an 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Redundancy interface management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/rdd', PID 4317,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Dynamic
flow capture service checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/dfcd', PID 4318,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
Connectivity fault management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/cfmd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/cfmd', PID 4319,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
address flooding and learning process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2ald'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2ald', PID 4320,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Layer 2
Control Protocol process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/l2cpd'
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30  starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30  starfire l2cp[4321]: Initialized 802.1X module and state machinesJan 20
17:09:30  starfire l2cp[4321]: Read acess profile () config
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/l2cpd', PID 4321,
status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: Multicast
Snooping process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/mcsnoopd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/mcsnoopd', PID
```

```
4325, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: commit
wrapup...
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress:
activating '/var/etc/ntp.conf'
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in progress: start ffp
activate
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30  starfire ffp[4326]: "dynamic-profiles": No change to profiles ..............
```

Forwarding Logs to the External Syslog Server

When the device running Junos OS is set up for an external syslog server, the TOE forwards copies of local logs to the external syslog server and retains local copies of all logs when the TOE is configured in event log mode. In stream log mode, all logs except traffic logs are stored locally and can be forwarded to an external syslog server, whereas traffic logs can only be forwarded to an external syslog server.

The connection between the device running Junos OS and the syslog server is established on an event basis depending on preconfiguration of what type of logs are forwarded from local to external. When the configured condition is met, the device sends local logs to the external syslog server.

RELATED DOCUMENTATION

Sample Syslog Server Configuration on a Linux System | 23

6
CHAPTER

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

The following section describes how to configure audit log options in the evaluated configuration.

Configuring Audit Log Options for SRX345, SRX345-DUAL-AC, and SRX380 Devices

To configure audit log options for SRX345, SRX345-Dual-AC, and SRX380 devices:

1. Specify the number of files to be archived in the system logging facility.

```
[edit system syslog]
root@host# set archive files 2
```

2. Specify the file in which to log data.

```
[edit system syslog]
root@host# set file syslog any any
```

3. Specify the size of files to be archived.

```
[edit system syslog]
root@host# set file syslog archive size 10000000
```

4. Log system messages in a structured format.

```
[edit system syslog]
root@host# set file syslog structured-data
```

5. Configure security log events in the audit log buffer.

```
[edit]
root@host# set security log cache
```

6. Specify how to process and export security logs.

```
[edit]
root@host# set security log mode event
```

RELATED DOCUMENTATION

Sample Code Audits of Configuration Changes | 33

Sample Code Audits of Configuration Changes

This sample code audits all changes to the configuration secret data and sends the logs to a file named **syslog:**

```
[edit system]
syslog {
    file syslog {
        authorization info;
        change-log info;
        interactive-commands info;
    }
}
```

This sample code expands the scope of the minimum audit to audit all changes to the configuration, not just secret data, and sends the logs to a file named **syslog:**

```
[edit system]
syslog {
    file syslog {
        any any;
        authorization info;
        change-log any;
        interactive-commands info;
        kernel info;
        pfe info;
    }
}
```

Example: System Logging of Configuration Changes

This example shows a sample configuration and makes changes to users and secret data. It then shows the information sent to the audit server when the secret data is added to the original configuration and committed with the `load` command.

```
[edit system]
location {
    country-code US;
    building B1;
}
...
login {
    message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
        user admin {
            uid 2000;
             class super-user;
        authentication {
            encrypted-password “$ABC123”;
               # SECRET-DATA
        }
    }
    password {
        format md5;
    }
}
radius-server 192.0.2.15 {
```

```
    secret “$ABC123” # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file syslog {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
...
...
```

The new configuration changes the secret data configuration statements and adds a new user.

```
user@host# show | compare
[edit system login user admin authentication]
-    encrypted-password “$ABC123”; # SECRET-DATA
+    encrypted-password “$ABC123”; # SECRET-DATA
[edit system login]
+    user admin2 {
+        uid 2001;
+        class operator;
+        authentication {
+            encrypted-password “$ABC123”;
                    # SECRET-DATA
+        }
+     }
[edit system radius-server 192.0.2.15]
-    secret “$ABC123”; # SECRET-DATA
+    secret “$ABC123”; # SECRET-DATA
```

RELATED DOCUMENTATION

Configuring Audit Log Options in the Evaluated Configuration | 32

CHAPTER 7

Configuring VPNs

Configuring VPN on a Device Running Junos OS

IN THIS SECTION

This section describes sample configurations of an IPsec VPN on a Junos OS device using the following IKE authentication methods:

Configuring VPN on a Device Running Junos OS Overview

IN THIS SECTION

This section describes sample configurations of an IPsec VPN on a Junos OS device using the following IKE authentication methods:

- "Configuring an IPsec VPN with a Preshared Key for IKE Authentication" on page 41
- "Configuring an IPsec VPN with an RSA Signature for IKE Authentication" on page 48
- "Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication" on page 52

Figure 1 on page 39 illustrates the VPN topology used in all the examples described in this section. Here, H0 and H1 are the host PCs, R0 and R2 are the two endpoints of the IPsec VPN tunnel, and R1 is a router to route traffic between the two different networks.

NOTE: The router R1 can be a Linux-based router, a Juniper Networks device, or any other vendor router.

Figure 1: VPN Topology

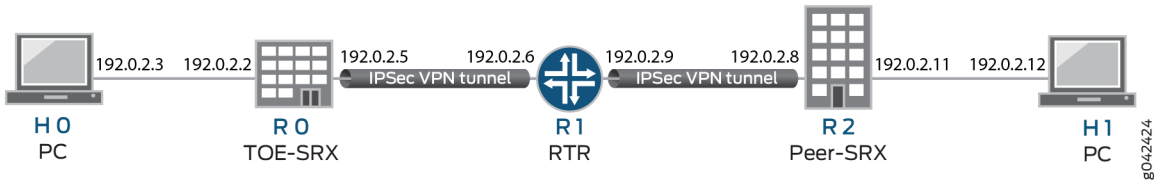

Table 1 on page 39 provides a complete list of the supported IKE protocols, tunnel modes, Phase 1 negotiation mode, authentication method or algorithm, encryption algorithm, DH groups supported for the IKE authentication and encryption (Phase1, IKE Proposal), and for IPsec authentication and encryption (Phase2, IPsec Proposal). The listed protocols, modes, and algorithms are supported and required for 20.4R1 Common Criteria.

Table 1: VPN Combination Matrix

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	pre-shared-keys	sha-256	group14	3des-cbc
IKEv2			rsa-signatures-2048	sha-384	group19	aes-128-cbc
			ecdsa-signatures-256		group20	aes-128-gcm
			ecdsa-signatures-384		group24	aes-192-cbc
						aes-256-cbc

Table 1: VPN Combination Matrix *(Continued)*

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
						aes-256-gcm

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha256-128	group14	ESP	aes-128-cbc
IKEv2				group19		aes-128-gcm
				group20		aes-192-cbc
				group24		aes-192-gcm
						aes-256-cbc
						aes-256-gcm

NOTE: The following sections provide sample configurations of IKEv1 IPsec VPN examples for selected algorithms. Authentication and encryption algorithms can be replaced in the configurations to accomplish the user's desired configurations. Use `set security ike gateway <gw-name> version v2-only` command for IKEv2 IPsec VPN.

Configuring an IPsec VPN with a Preshared Key for IKE Authentication

In this section, you configure devices running Junos OS for IPsec VPN using a preshared key as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption is shown in Table 2 on page 41

Table 2: IKE or IPsec Authentication and Encryption

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	pre-shared-keys	sha-256	group14	aes-256-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha-256-128	group14	ESP	aes-256-cbc

NOTE: A device running Junos OS uses certificate-based authentication or preshared keys for IPsec. TOE accepts ASCII preshared or bit-based keys up to 255 characters (and their binary equivalents) that contain uppercase and lowercase letters, numbers, and special characters such as !, @, #, $, %, ^, &, *, (, and). The device accepts the preshared text keys and converts the text string into an authentication value as per RFC 2409 for IKEv1 or RFC 4306 for IKEv2, using the PRF that is configured as the hash algorithm for the IKE exchanges. The Junos OS does not impose minimum complexity requirements for preshared keys. Hence, users are advised to carefully choose long preshared keys of sufficient complexity.

Configuring IPsec VPN with Preshared Key as IKE Authentication on the Initiator

To configure the IPsec VPN with preshared key IKE authentication on the initiator:

1. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method pre-shared-keys
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha256
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

   Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

2. Configure the IKE policy.

```
[edit]
user@host# set security ike policy ike-policy1 mode main
user@host# set security ike policy ike-policy1 proposals ike-proposal1
user@host# prompt security ike policy ike-policy1 pre-shared-key ascii-text
New ascii-text (secret):
Retype new ascii-text (secret):
```

   Here, `ike-policy1` is the IKE policy name and `ike-proposal1` is the IKE proposal name given by the authorized administrator.
   You must enter and reenter the preshared key when prompted. For example, the preshared key can be *CertSqa@jnpr2014*.

   The preshared key can alternatively be entered in hexadecimal format. For example:

```
[edit]
user@host# prompt security ike policy ike-policy1 pre-shared-key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

   Here, the hexadecimal preshared key can be `cc2014bae9876543`.

3. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set security proposal ipsec-proposal1 protocol esp
user@host# set security proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set security proposal ipsec-proposal1 encryption-algorithm aes-256-cbc
```

   Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

4. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set security policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set security policy ipsec-policy1 proposals ipsec-proposal1
```

Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

5. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface ge-0/0/2
```

Here, `gw1` is an IKE gateway name, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following additional configuration is also needed in the case of IKEv2

6. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0 preference
1
```

Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

7. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
```

```
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

8. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-close
```

Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

9. Commit your configuration.

```
user@host# commit
```

Configuring IPsec VPN with Preshared Key as IKE Authentication on the Responder

To configure the IPsec VPN with preshared key IKE authentication on the responder:

1. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method pre-shared-keys
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha256
user@host# set proposal ike-proposal1 encryption-algorithm 3des-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

2. Configure the IKE policy.

```
[edit]
user@host# set security ike policy ike-policy1 mode main
user@host# set security ike policy ike-policy1 proposals ike-proposal1
```

NOTE: Here, `ike-policy1` is the IKE policy name and `ike-proposal1` is the IKE proposal name given by the authorized administrator.

```
user@host# prompt security ike policy ike-policy1 pre-shared-key ascii-text
New ascii-text (secret):
Retype new ascii-text (secret):
```

NOTE: You must enter and reenter the preshared key when prompted. For example, the preshared key can be *CertSqa@jnpr2014*.

NOTE: The pre-share key could alternatively be entered in hexadecimal format. For example,

```
user@host# prompt security ike policy ike-policy1 pre-shared-key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

Here, the hexadecimal preshared key can be `cc2014bae9876543`.

3. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set proposal ipsec-proposal1 encryption-algorithm 3des-cbc
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

4. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

5. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.5
user@host# set gateway gw1 local-identity inet 192.0.2.8
user@host# set gateway gw1 external-interface ge-0/0/2
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.5` is the peer VPN endpoint IP, `192.0.2.8` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following additional configuration is also needed in the case of IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

6. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.7/24 qualified-next-hop st0.0 preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

7. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

8. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

9. Commit your configuration.

```
user@host# commit
```

Configuring an IPsec VPN with an RSA Signature for IKE Authentication

The following section provides an example to configure Junos OS devices for IPsec VPN using RSA Signature as IKE Authentication method, whereas, the algorithms used in IKE/IPsec authentication/ encryption is as shown in the following table. In this section, you configure devices running Junos OS for IPsec VPN using an RSA signature as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption is shown in Table 3 on page 48.

Table 3: IKE/IPsec Authentication and Encryption

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	rsa-signatures-2048	sha-256	group19	aes-128-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	hmac-sha-256-128	group19	ESP	aes-128-cbc

Configuring IPsec VPN with RSA Signature as IKE Authentication on the Initiator or Responder

To configure the IPsec VPN with RSA signature IKE authentication on the initiator:

1. Configure the PKI. See Example: Configuring PKI.
2. Generate the RSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load the CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load the CRL. See Example: Manually Loading a CRL onto the Device .
5. Generate and load a local certificate. See Example: Loading CA and Local Certificates Manually.

6. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method rsa-signatures
user@host# set proposal ike-proposal1 dh-group group19
user@host# set proposal ike-proposal1 authentication-algorithm sha-256
user@host# set proposal ike-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: Here, `ike-proposal1` is the name given by the authorized administrator.

7. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

NOTE: Here, `ike-policy1` IKE policy name given by the authorized administrator.

8. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 authentication-algorithm hmac-sha-256-128
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-128-cbc
```

NOTE: Here, `ipsec-proposal1` is the name given by the authorized administrator.

9. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group19
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the name given by the authorized administrator.

10. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface fe-0/0/1
```

NOTE: Here, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `fe-0/0/1` is the local outbound interface as VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

11. Configure VPN.

```
[edit security ipsec]
user@host# set vpn vpn1 ike gateway gw1
user@host# set vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set vpn vpn1 bind-interface st0.0
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

```
[edit]
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0
preference 1
```

12. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zone and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

14. Commit the configuration.

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

Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication

In this section, you configure devices running Junos OS for IPsec VPN using an ECDSA signature as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption are shown in Table 4 on page 52.

Table 4: IKE or IPsec Authentication and Encryption

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 1 Proposal (P1, IKE)			
			Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
IKEv1	Main	Route	ecdsa-signatures-256	sha-384	group14	aes-256-cbc

IKE Protocol	Tunnel Mode	Phase1 Negotiation Mode	Phase 2 Proposal (P2, IPsec)			
			Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
IKEv1	Main	Route	No Algorithm	group14	ESP	aes-256-gcm

Configuring IPsec VPN with ECDSA signature IKE authentication on the Initiator

To configure the IPsec VPN with ECDSA signature IKE authentication on the initiator:

1. Configure the PKI. See Example: Configuring PKI.
2. Generate the RSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load the CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load the CRL. See Example: Manually Loading a CRL onto the Device .
5. Generate and load a local certificate. See Example: Loading CA and Local Certificates Manually.

6. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha-384
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

7. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

8. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

9. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

10. Configure IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.8
user@host# set gateway gw1 local-identity inet 192.0.2.5
user@host# set gateway gw1 external-interface ge-0/0/2
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.8` is the peer VPN endpoint IP, `192.0.2.5` is the local VPN endpoint IP, and `ge-0/0/2` is a local outbound interface as the VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

11. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.10/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

12. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
```

```
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

14. Commit your configuration.

```
user@host# commit
```

Configuring IPsec VPN with ECDSA signature IKE authentication on the Responder

To configure IPsec VPN with ECDSA signature IKE authentication on the responder:

1. Configure the PKI. See Example: Configuring PKI.

2. Generate the ECDSA key pair. See Example: Generating a Public-Private Key Pair.
3. Generate and load the CA certificate. See Example: Loading CA and Local Certificates Manually.
4. Load the CRL. See Example: Manually Loading a CRL onto the Device .
5. Configure the IKE proposal.

```
[edit security ike]
user@host# set proposal ike-proposal1 authentication-method ecdsa-signatures-256
user@host# set proposal ike-proposal1 dh-group group14
user@host# set proposal ike-proposal1 authentication-algorithm sha-384
user@host# set proposal ike-proposal1 encryption-algorithm aes-256-cbc
```

NOTE: Here, `ike-proposal1` is the IKE proposal name given by the authorized administrator.

6. Configure the IKE policy.

```
[edit security ike]
user@host# set policy ike-policy1 mode main
user@host# set policy ike-policy1 proposals ike-proposal1
user@host# set policy ike-policy1 certificate local-certificate cert1
```

7. Configure the IPsec proposal.

```
[edit security ipsec]
user@host# set proposal ipsec-proposal1 protocol esp
user@host# set proposal ipsec-proposal1 encryption-algorithm aes-256-gcm
```

NOTE: Here, `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

8. Configure the IPsec policy.

```
[edit security ipsec]
user@host# set policy ipsec-policy1 perfect-forward-secrecy keys group14
user@host# set policy ipsec-policy1 proposals ipsec-proposal1
```

NOTE: Here, `ipsec-policy1` is the IPsec policy name and `ipsec-proposal1` is the IPsec proposal name given by the authorized administrator.

9. Configure the IKE.

```
[edit security ike]
user@host# set gateway gw1 ike-policy ike-policy1
user@host# set gateway gw1 address 192.0.2.5
user@host# set gateway gw1 local-identity inet 192.0.2.8
user@host# set gateway gw1 external-interface ge-0/0/1
```

NOTE: Here, `gw1` is an IKE gateway name, `192.0.2.5` is the peer VPN endpoint IP, `192.0.2.8` is the local VPN endpoint IP, and `ge-0/0/1` is a local outbound interface as the VPN endpoint. The following configuration is also needed for IKEv2.

```
[edit security ike]
user@host# set gateway gw1 version v2-only
```

10. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 192.0.2.1/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `vpn1` is the VPN tunnel name given by the authorized administrator.

11. Configure the outbound flow policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

12. Configure the inbound flow policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application any
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then permit
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-
close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

13. Commit your configuration.

```
user@host# commit
```

SEE ALSO

- IPsec VPN Feature Guide for Security Devices
- Understanding a Security Flow Policy on a Device Running Junos OS

8
CHAPTER

Configuring Security Flow Policies

Understanding a Security Flow Policy on a Device Running Junos OS

IN THIS SECTION

Security Flow Policy on a Device Running Junos OS Overview

IN THIS SECTION

You can define a security flow policy on a device running Junos OS to inspect and process network packets. The device can permit, deny, and log operations to be associated with each policy. Each of these policies are associated to zones on which distinct network interfaces are bound.

The following modes can be defined for a security flow policy to determine how a device directs traffic:

- Bypass—The `Permit` option directs the traffic traversing the device through the stateful firewall inspection, but not through the IPsec VPN tunnel.
- Discard—The `Deny` option inspects and drops all packets that do not match any `Permit` policies.
- Protect—The traffic is routed through an IPsec tunnel based on the combination of route lookup and `Permit` policy inspection.
- Log—This option logs traffic and session information for all the modes mentioned above.

The following sections describe how to configure a security policy for each of these modes:

- "Configuring a Security Flow Policy in Firewall Bypass Mode" on page 62

Configuring a Security Flow Policy in Firewall Bypass Mode

To configure a security flow policy for firewall bypass mode:

- Configure the security policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses. `junos-ssh` is an example of a Junos OS default predefined application that can be configured in a security policy to enforce SSH traffic.

Configuring a Security Policy in Firewall Discard Mode

To configure a security flow policy for firewall discard mode:

- Configure the security policies.

```
[edit security policies]
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match source-address
untrustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match destination-
address trustLan
user@host# set from-zone untrustZone to-zone trustZone policy policy1 match application junos-
telnet
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then deny
```

```
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then log session-init
user@host# set from-zone untrustZone to-zone trustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are the preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses. `junos-telnet` is an example of a Junos OS default predefined application that can be configured in a security policy to enforce Telnet traffic.

Configuring a Security Flow Policy in IPsec Protect Mode

To configure a security flow policy for IPsec protect mode:

1. Configure the VPN.

```
[edit]
user@host# set security ipsec vpn vpn1 ike gateway gw1
user@host# set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
user@host# set security ipsec vpn vpn1 bind-interface st0.0
user@host# set routing-options static route 198.51.100.14/24 qualified-next-hop st0.0
preference 1
```

NOTE: Here, `gw1` and `ipsec-policy1` are preconfigured IKE and IPsec policies.

2. Configure the security policies.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application any
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

> **NOTE**: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

For more information on stateful session behavior, see Traffic Processing on SRX Series Devices Overview

For more information on how to configure known good and bad lists, see Configuring Security Policies

For more information on scheduling security policies, see Scheduling Security Policies and Policer Implementation Overview

SEE ALSO

- Configuring VPN on a Device Running Junos OS

CHAPTER 9

Configuring Traffic Filtering Rules

Overview

By default, the TOE denies all traffic through an SRX Series device. In fact, an implicit default security policy exists that denies all packets. You can change this behavior by configuring a standard security policy that permits certain types of traffic. The implicit default policy can be changed to permit all traffic with the `set security policies default-policy` command; however, this is not recommended.

The security policy rule set is an ordered list of security policy entries enforced by the firewall rules, each of which contains the specification of a network flow and an action:

- Source IP address and network mask
- Destination IP address and network mask
- Protocol
- Source port
- Destination port
- Action: permit, deny, drop silently, log

Each packet is compared against entries in the security policy rule set in sequential order until one is found that matches the specification in the policy, or until the end of the rule set is reached, in which case the implicit default policy is implemented and the packet is discarded.

RELATED DOCUMENTATION

Reordering Security Policies

Understanding Protocol Support

You can configure the devices running Junos OS to perform stateful network traffic filtering on network packets using network traffic protocols and network fields as described in Table 5 on page 67.

Table 5: Network Traffic Protocols and Fields

Protocol or RFC	Fields
ICMPv4 - RFC 792, Internet Control Message Protocol version 4	• Type • Code
ICMPv6 - RFC 4443, Internet Control Message Protocol version 6	• Type • Code
IPv4 - RFC 791, Internet Protocol	• Source address • Destination address • Transport Layer Protocol
IPv6 - RFC 2460, Internet Protocol	• Source address • Destination address • Transport Layer Protocol
TCP - RFC 793, Transmission Control Protocol	• Source port • Destination port
UDP - RFC 768, User Datagram Protocol	• Source port • Destination port

The following protocols are also supported on devices running Junos OS and are a part of this evaluation.

- IPsec
- IKE
- SSH

The following protocols are supported on devices running Junos OS but are not included in the scope of this evaluation.

- OSPF
- BGP
- RIP

RELATED DOCUMENTATION

Configuring Traffic Filter Rules | 68

Configuring Traffic Filter Rules

Traffic filter rules can be configured on a device to enforce validation against protocols attributes and direct traffic accordingly to the configured attributes. These rules are based on zones on which network interfaces are bound.

The following procedure describes how to configure traffic filter rules to direct FTP traffic from source `trustZone` to destination `untrustZone` and from source network `trustLan` to destination network `untrustLan`. Here, traffic is traversing from the devices interface A on `trustZone` to interface B on `untrustZone`.

1. Configure a zone and its interfaces.

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

2. Configure the security policy in the specified zone-to-zone direction and specify the match criteria.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match source-address
trustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match destination-
address untrustLan
user@host# set from-zone trustZone to-zone untrustZone policy policy1 match application ftp
```

3. Configure the security policy in the specified zone-to-zone direction and specify the action to take when a packet matches a criteria.

```
[edit security policies]
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then permit
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then log session-init
user@host# set from-zone trustZone to-zone untrustZone policy policy1 then session-close
```

NOTE: Here, `trustZone` and `untrustZone` are preconfigured security zones and `trustLan` and `untrustLan` are preconfigured network addresses.

RELATED DOCUMENTATION

Understanding Protocol Support | 66

Configuring Default Deny-All and Reject Rules

By default, security devices running Junos OS deny traffic unless rules are explicitly created to allow it using the following command:

```
[edit]
user@host#set security policies default-policy deny-all
```

You can configure your security devices running Junos OS to enforce the following default reject rules with logging on all network traffic:

- Invalid fragments
- Fragmented IP packets that cannot be reassembled completely
- Where the source address is equal to the address of the network interface
- Where the source address does not belong to the networks associated with the network interface
- Where the source address is defined as being on a broadcast network
- Where the source address is defined as being on a multicast network

- Where the source address is defined as being a loopback address
- Where the source address is a multicast packet
- Where the source or destination address is a link-local address
- Where the source or destination address is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4
- Where the source or destination address is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6
- With the IP option Loose Source Routing, Strict Source Routing, or Record Route is specified

Logging the Dropped Packets Using Default Deny-all Option

The evaluated configuration device drops all IPv6 traffic by default. This topic describes how to log packets dropped by this default deny-all option.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 20.4R1 and edit the configuration.

> **NOTE**: You can enter the configuration commands in any order and commit all the commands at once.

To log packets dropped by the default deny-all option:

1. Configure a network security policy in a global context and specify the security policy match criteria.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log match source-address any
destination-address any application any
```

2. Specify the policy action to take when the packet matches the criteria.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log then deny
```

3. Configure the security policy to enable logs at the session initialization time.

```
[edit security policy]
user@host# set global policy always-last-default-deny-and-log then log session-init
```

NOTE: This procedure might capture a very large amount of data until you have configured the other policies.

To permit all IPv6 traffic into an SRX Series device, configure the device with flow-based forwarding mode. While the default policy in flow-based forwarding mode is still to drop all IPv6 traffic, you can now add rules to permit selected types of IPv6 traffic.

```
user@host# set security forwarding-options family inet6 mode flow-based
```

Configuring Mandatory Reject Rules for Invalid Fragments and Fragmented IP Packets

This topic describes how to configure mandatory reject rules for invalid fragments and fragmented IP packets that cannot be reassembled.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 20.4R1 and edit the configuration.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure mandatory reject rules:

1. Specify the flow configuration to forcefully reassemble the IP fragments.

```
[edit]
user@host# set security flow force-ip-reassembly
```

2. Delete the screen ID and the IDS options and enable the ICMP fragment IDS option.

```
[edit]
user@host# delete security screen ids-option trustScreen icmp fragment
```

3. Delete the IP layer IDS option and enable the IP fragment blocking IDS option.

```
[edit]
user@host# delete security screen ids-option trustScreen ip block-frag
```

Configuring Default Reject Rules for Source Address Spoofing

The following guidelines describe when to configure the default reject rules for source address spoofing:

- When the source address is equal to the address of the network interface where the network packet was received.
- When the source address does not belong to the networks associated with the network interface where the network packet was received.
- When the source address is defined as being on a broadcast network.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 20.2R1and edit the configuration.

NOTE: You can enter the configuration commands in any order and commit all the commands at once.

To configure default reject rules to log source address spoofing:

1. Configure the security screen features and enable the IP address spoofing IDS option.

```
[edit]
user@host# set security screen ids-option trustScreen ip spoofing
```

2. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

Configuring Default Reject Rules with IP Options

This topic describes how to configure default reject rules with IP options. The IP options enable the device to either block any packets with loose or strict source route options or detect such packets and then record the event in the counters list for the ingress interface.

1. Before you begin, log in with your root account to an SRX Series device running Junos OS Release 20.2R1.

> **NOTE**: You can enter the configuration commands in any order and commit all the commands at once.

To configure the default reject rules with IP options:

1. Configure the screen features to enable IP options.

```
[edit security screen ids-option trustScreen]
user@host# set ip source-route-option
user@host# set ip loose-source-route-option
user@host# set ip strict-source-route-option
user@host# set ip record-route-option
```

2. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

Configuring Default Reject Rules

The following guidelines describe when to configure the default reject rules:

- Source address is defined on a multicast network, a loopback address, or a multicast address.
- The source or destination address of a packet is a link-local address, an address “reserved for future use” as specified in RFC 5735 for IPv4, an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6.
- An illegal or out-of-sequence TCP packet is received.

1. Before you begin, log in with your root account on a Junos OS device running Junos OS Release 20.4R1 and edit the configuration.

> **NOTE**: You can enter the configuration commands in any order and commit all the commands at once.

To configure default reject rules:

1. Configure the security screen features and enable the IP address spoofing IDS option.

```
[edit]
user@host# set security screen ids-option trustScreen ip spoofing
```

2. Configure the security flow feature to log the dropped illegal packets.

```
[edit]
user@host# set security flow log dropped-illegal-packet
```

3. Configure the rule to block reserved addresses.

```
[edit]
user@host# set security flow advanced-options drop-matching-reserved-ip-address
```

NOTE: After running the set security flow advanced-options drop-matching-reserved-ip-address command, you must create a neighbor cache entry on each host on a local link to the SRX device. For example, on a Linux host you would enter the following command: `ip -6 neigh add 2001:db8:c18:1::2 lladdr 2c:6b:f5:69:ce:00 dev eth1` where, `2001:db8:c18:1::2` is the IPv6 address of the adjacent SRX interface, and `2c:6b:f5:69:ce:00` is the MAC address of the adjacent SRX interface.You will also need to create neighbor cache entries on the SRX device for all hosts on the local link, as shown in the following example:

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet6 {
                address 2001:db8:c18:1::2/64 {
                    ndp 2001:db8:c18:1::3 mac 00:0c:29:97:70:a5;
                }
            }
        }
    }
}
```

In the example, `2001:db8:c18:1::2` is the IPv6 address of the SRX ge-0/0/0 interface, `2001:db8:c18:1::3` is a host on the local link, and `00:0c:29:97:70:a5` is the MAC address of that host.

4. Specify the name of the security zone and the IDS option object applied to the zone.

```
[edit]
user@host# set security zones security-zone trustZone screen trustScreen
```

5. Configure the mandatory TCP reject rule.

```
[edit]
user@host# set security flow tcp-session strict-syn-check
```

CHAPTER 10

Configuring Network Attacks

Configuring IP Teardrop Attack Screen

This topic describes how to configure detection of an IP teardrop attack.

Teardrop attacks exploit the reassembly of fragmented IP packets. In the IP header, one of the field is the fragment offset fields, which indicates the starting position, or offset of the data contained in a fragmented packet, relative to the data of the original unfragmented packet. When the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap and the server attempting to reassemble the packet might crash.

To enable detection of a teardrop attack:

1. Configure interfaces and assign IP addresses to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
```

```
permit
user@host# set security policies default-policy deny-all
```

4. Configure the security screen option and attach it to the **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen ip tear-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring TCP Land Attack Screen

This topic describes how to configure detection of a TCP land attack.

Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and the source IP address.

To enable detection of a TCP land attack:

1. Configure interfaces and assign IP addresses to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp land
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring ICMP Fragment Screen

This topic describes how to configure detection of an ICMP fragment attack.

If an ICMP packet is large, then it must be fragmented. When the ICMP fragment protection screen option is enabled, the Junos OS blocks any ICMP packet that has many fragment flags set or that has an offset value indicated in the offset field.

To enable detection of an ICMP fragment IDS attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp fragment
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring Ping-Of-Death Attack Screen

This topic describes how to configure detection of ping-of-death attack.

The IP datagram with the protocol field of the IP header is set to 1 (ICMP), the last fragment bit is set, and (IP offset * 8) + (IP data length) > 65535. The IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.

To enable detection of a ping-of-death IDP attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

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

```
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp ping-death
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring tcp-no-flag Attack Screen

This topic describes how to configure detection of a `tcp-no-flag` attack.

A TCP segment with no control flags set is an anomalous event causing various responses from the recipient. When the TCP no-flag is enabled, the device detects the TCP segment headers with no flags set, and drops all TCP packets with missing or malformed flag fields.

To enable detection of a `tcp-no-flag` option:

1. Configure interfaces and assign an IP address to the interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp tcp-no-flag
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

Configuring TCP SYN-FIN Attack Screen

This topic describes how to configure detection of a TCP SYN-FIN attack.

A TCP header with the SYN and FIN flags set is anomalous TCP behavior causing various responses from the recipient, depending on the OS. Blocking packets with SYN and FIN flags helps prevent the OS system probes.

To enable detection of TCP SYN-FIN bits:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp syn-fin
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring TCP fin-no-ack Attack Screen

This topic describes how to configure detection of TCP `fin-no-ack` attack. A TCP header with the FIN flag set but not the ACK flag is anomalous TCP behavior.

To enable detection of FIN bits with no ACK bit IDS option:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones **trustZone** and **untrustZone** and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from **untrustZone** to **trustZone**.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to **untrustZone**.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp fin-no-ack
user@host# set security zones security-zone untrustZone screen untrustScreen
user@host# set security screen ids-option untrustScreen alarm-without-drop
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring UDP Bomb Attack Screen

If the UDP length specified is less than the IP length specified then the malformed packet type is associated with a denial-of-service attempt. By default, SRX drops these packets. No configuration is required.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring UDP CHARGEN DoS Attack Screen

This topic describes how to configure protection from a UDP CHARGEN DoS attack.

NOTE: UDP packet is detected with a source port of 7 and a destination port of 19 is an attack.

To enable detection of a UDP CHARGEN DoS attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to the `trustZone` with the Junos OS predefined application `junos-chargen`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application junos-chargen
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
deny
user@host# set security policies default-policy permit-all
```

4. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

5. To allow the packet to reach the destination, change the policy configuration from `deny` to `permit`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | **104**

Configuring TCP SYN and RST Attack Screen

This topic describes how to configure TCP packet when the SYN and RST flags are set.

To enable detection of a TCP SYN and RST attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` the `untrustZone` and assign interfaces to them.

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

```
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure the IDP custom-attack signatures.

```
[edit]
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match destination-
address any
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match application default
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 match attacks custom-
attacks syn_rst
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 then action no-action
user@host# set security idp idp-policy idpengine rulebase-ips rule 1 then notification log-
attacks
user@host# set security idp active-policy idpengine
user@host# set security idp custom-attack syn_rst severity info
user@host# set security idp custom-attack syn_rst attack-type signature context packet
user@host# set security idp custom-attack syn_rst attack-type signature pattern
user@host# set security idp custom-attack syn_rst attack-type signature direction any
user@host# set security idp custom-attack syn_rst attack-type signature protocol tcp tcp-
flags rst
user@host# set security idp custom-attack syn_rst attack-type signature protocol tcp tcp-
flags syn
```

4. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit application-services idp
user@host# set security policies default-policy deny-all
```

5. Configure security `tcp-session` option in flow.

```
[edit]
user@host# set security flow tcp-session no-syn-check
user@host# set security flow tcp-session no-sequence-check
```

6. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

7. To allow the traffic to reach the destination, configure the `tcp-session` option.

```
[edit]
user@host# set security flow tcp-session relax-check
```

8. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring ICMP Flood Attack Screen

This topic describes how to configure detection of an ICMP flood attack.

An ICMP flood typically occurs when an ICMP echo request overloads the victim with many requests such that the ICMP echo request spends all its resources responding until it can no longer process valid network traffic. When enabling the ICMP flood protection feature, you can set a threshold that, once exceeded, invokes the ICMP flood attack protection feature.

To enable detection of an ICMP flood attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to `untrustZone`.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp flood
```

```
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring TCP SYN Flood Attack Screen

This topic describes how to configure detection of a TCP SYN flood attack.

A SYN flood occurs when a host is so overwhelmed by SYN segments initiating incomplete connection requests that it can no longer process legitimate connection requests.

To enable detection of a TCP SYN flood attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones trustZone and untrustZone and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from untrustZone to trustZone.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp syn-flood
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
```

```
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring TCP Port Scan Attack Screen

This topic describes how to configure detection of a TCP port scan attack.

A port scan occurs when one source IP address sends an IP packet containing TCP SYN segments to a defined number of different ports at the same destination IP address within a defined interval.

To enable detection of a TCP port scan attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from untrustZone to trustZone.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to untrustZone.

```
[edit]
user@host# set security screen ids-option untrustScreen tcp port-scan
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring UDP Port Scan Attack Screen

This topic describes how to configure detection of a UDP port scan attack.

These attacks scan the target IP addresses for open, listening, or responsive services by targeting multiple protocols or ports on one or more target IP address using obvious (sequentially numbered) patterns of the target protocol or port numbers. The patterns are derived by randomizing the protocol or port numbers and randomizing the time delays between the transmissions.

To enable detection of a UDP port scan attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to `untrustZone`.

```
[edit]
user@host# set security screen ids-option untrustScreen udp port-scan
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

Configuring IP Sweep Attack Screen

This topic describes how to configure detection of an IP sweep attack.

An address sweep occurs when one source IP address sends a defined number of ICMP packets to different hosts within a defined time interval (5000 microseconds is the default value). The purpose of this attack is to send ICMP packets—typically echo requests—to various hosts in the hope that at least one replies, thus uncovering an address to target.

To enable detection of an IP sweep attack:

1. Configure interfaces and assign an IP address to interfaces.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 198.51.100.0/24
```

2. Configure security zones `trustZone` and `untrustZone` and assign interfaces to them.

```
[edit]
user@host# set security zones security-zone trustZone host-inbound-traffic system-services all
user@host# set security zones security-zone trustZone host-inbound-traffic protocols all
user@host# set security zones security-zone trustZone interfaces ge-0/0/1.0
user@host# set security zones security-zone untrustZone host-inbound-traffic system-services
all
user@host# set security zones security-zone untrustZone host-inbound-traffic protocols all
user@host# set security zones security-zone untrustZone interfaces ge-0/0/3.0
```

3. Configure security policies from `untrustZone` to `trustZone`.

```
[edit]
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
source-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
destination-address any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 match
application any
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
permit
user@host# set security policies default-policy deny-all
```

4. Configure security screens and attach them to `untrustZone`.

```
[edit]
user@host# set security screen ids-option untrustScreen icmp ip-sweep
user@host# set security screen ids-option untrustScreen alarm-without-drop
user@host# set security zones security-zone untrustZone screen untrustScreen
```

5. Configure syslog.

```
[edit]
user@host# set system syslog file syslog any any
user@host# set system syslog file syslog archive size 10000000
user@host# set system syslog file syslog structured-data
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-init
user@host# set security policies from-zone untrustZone to-zone trustZone policy policy1 then
log session-close
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

CHAPTER 11

Configuring the IDP Extended Package

IDP Extended Package Configuration Overview

The Junos OS Intrusion Detection and Prevention (IDP) policy enables you to selectively enforce various attack detection and prevention techniques on network traffic passing through an IDP-enabled device. It allows you to define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

An IDP policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network.

A policy is made up of rule bases, and each rule base contains a set of rules. You define rule parameters, such as traffic match conditions, action, and logging requirements, then add the rules to rule bases. After you create an IDP policy by adding rules in one or more rule bases, you can select that policy to be the active policy on your device.

To configure the IDP extended package (IPS-EP) perform the following steps:

1. Enable IPS in a security policy. See IDP Policy Rules and IDP Rule Bases.
2. Configure IDP policy rules, IDP rule bases, and IDP rule actions. See IDP Policy Rules and IDP Rule Bases.
3. Configure IDP custom signatures. See Understanding IDP Signature-Based Attacks.
4. Update the IDP signature database. See Updating the IDP Signature Database Overview.
5. When the IDP hits a resource limit, the default behavior is to ignore the flow and let the flow pass without inspection. To avoid this behavior, configure the `drop-on-limit` option.
   This command ensures IDP attack inspection of all traffic and does not allow any traffic without inspection.

   ```
   [edit]
   user@host# set security idp sensor-configuration flow drop-on-limit
   ```

   Also, see IDP Sensor Configuration.

RELATED DOCUMENTATION

- Intrusion Detection and Prevention Feature Guide

12
CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests

IN THIS SECTION

The cryptographic module enforces security rules to ensure that a device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode of operation meets the security requirements of FIPS 140-2 Level 2. To validate the output of cryptographic algorithms approved for FIPS and test the integrity of some system modules, the device performs the following series of known answer test (KAT) self-tests:

- `kernel_kats`—KAT for kernel cryptographic routines
- `md_kats`—KAT for libmd and libc
- `openssl_kats`—KAT for OpenSSL cryptographic implementation
- `quicksec_7_0_kats`—KAT for Quicksec Toolkit cryptographic implementation
- `octcrypto_kats`—KAT for Octeon
- `JSF_Crypto_(Octeon)_KATS`—KAT for JSF crypto octeon

The KAT self-tests are performed automatically at startup and reboot, when FIPS mode of operation is enabled on the device. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and ECDSA key pairs, and manually entered keys.

If the KATs are completed successfully, the system log (syslog) file is updated to display the tests that were executed.

If the device fails a KAT, the device writes the details to a system log file, enters FIPS error state (panic), and reboot.

The `file show /var/log/messages` command displays the system log.

Proceed with normal operation after the reboot is complete. If an error occurs, please contact the Juniper Networks Technical Assistance Center (JTAC).

Performing Power-On Self-Tests on the Device

Each time the cryptographic module is powered on, the module tests that the cryptographic algorithms still operate correctly and that sensitive data has not been damaged. Power-on self-tests are performed on demand by power cycling the module.

On powering on or resetting the device, the module performs the following self-tests. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fail, the module enters the Critical Failure error state.

If the device fails a KAT, the device writes the details to a system log file, enters FIPS error state (panic), and reboots.

The module displays the following status output for SRX345, SRX345-DUAL-AC, and SRX380 devices while running the power-on self-tests:

```
Verified jboot signed by PackageDevelopmentECP256_2020 method ECDSA256+SHA256 Verified junos
signed by PackageDevelopmentECP256_2020 method ECDSA256+SHA256
veriexec: cannot update veriexec for /usr/lib/libext_db.so.3: Too many links
veriexec: cannot update veriexec for /usr/lib/libpsu.so.3: Too many links
veriexec: cannot update veriexec for /usr/lib/libxml2.so.3: Too many links
veriexec: cannot update veriexec for /usr/lib/libyaml.so.3: Too many links
veriexec: cannot update veriexec for /var/jailetc/mime.types: No such file or directory
veriexec: cannot update veriexec for /var/jailetc/php_mod.ini: No such file or directory
Verified junos-20.4R1 signed by PackageDevelopmentECP256_2020 method ECDSA256+SHA256 Checking
integrity of BSD labels:
  s1: Passed
  s2: Passed
  s3: Passed
  s4: Passed
** /dev/bo0s3e
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 599646 free (30 frags, 74952 blocks, 0.0% fragmentation)
** /dev/bo0s3f
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 18789959 free (471 frags, 2348686 blocks, 0.0% fragmentation) Checking integrity of
licenses:
  DemoLabJUNOS634993695.lic: No recovery data
  DemoLabJUNOS747689902.lic: No recovery data
  DemoLabJUNOS867795690.lic: No recovery data Checking integrity of configuration:
  rescue.conf.gz: No recovery data
LPC bus driver
lpcbus0 on cpld0
```

```
tpm0: <Trusted Platform Module>on lpcbus0
tpm: IFX SLB 9660 TT 1.2 rev 0x10
Loading configuration ...
mgd: warning: schema: dbs_remap_daemon_index: could not find daemon name 'ikemd'
mgd: Running FIPS Self-tests
mgd: Testing JSF Crypto (Octeon) KATs:
mgd:   AES-CBC Known Answer Test:                       Passed
mgd:   AES-GCM Known Answer Test:                       Passed
mgd:   RSA-SIGN Known Answer Test:                      Passed
mgd:   ECDSA-SIGN Known Answer Test:                    Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test:    Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:            Passed
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   SHA-2-384 Known Answer Test:                     Passed
mgd:   SHA-2-512 Known Answer Test:                     Passed
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd: Testing MACSec KATS:
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES256-CMAC Known Answer Test:                   Passed
mgd:   AES-ECB Known Answer Test:                       Passed
mgd:   AES-KEYWRAP Known Answer Test:                   Passed
mgd:   KBKDF Known Answer Test:                         Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   SHA-2-512 Known Answer Test:                     Passed
mgd: Testing Octeon KATS:
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd: Testing OpenSSL KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   FIPS ECDSA Known Answer Test:                    Passed
mgd:   FIPS ECDH Known Answer Test:                     Passed
mgd:   FIPS RSA Known Answer Test:                      Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
```

```
mgd:   HMAC-SHA2-224 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-512 Known Answer Test:                 Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd:   AES-GCM Known Answer Test:                       Passed
mgd:   ECDSA-SIGN Known Answer Test:                    Passed
mgd:   KDF-IKE-V1 Known Answer Test:                    Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:                Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test:    Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:            Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-224 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-512 Known Answverieexec: no fingerprint for file='/sbin/kats/cannot-exec'
fsid=83 fileid=5048524 gen=1 uid=0 pid=1073
er Test:                 Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd:   AES-GCM Known Answer Test:                       Passed
mgd:   SSH-RSA-ENC Known Answer Test:                   Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:   SSH-ECDSA-SIGN Known Answer Test:                Passed
mgd:   KDF-IKE-V1 Known Answer Test:                    Passed
mgd:   KDF-IKE-V2 Known Answer Test:                    Passed
mgd: Testing QuickSec KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-224 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-512 Known Answer Test:                 Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd:   AES-GCM Known Answer Test:                       Passed
mgd:   SSH-RSA-ENC Known Answer Test:                   Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:   KDF-IKE-V1 Known Answer Test:                    Passed
mgd:   KDF-IKE-V2 Known Answer Test:                    Passed
mgd: Testing SSH IPsec KATS:
```

```
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd:   SSH-RSA-ENC Known Answer Test:                   Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:   KDF-IKE-V1 Known Answer Test:                    Passed
mgd: Testing file integrity:
mgd:   File integrity Known Answer Test:                Passed
mgd: Testing crypto integrity:
mgd:   Crypto integrity Known Answer Test:              Passed
mgd: Expect an exec Authentication error...
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed
```

NOTE: The module implements cryptographic libraries and algorithms that are not utilized in the approved mode of operation.

The module displays the following status output for SRX345 and SRX380 devices while failure of the power-on self-tests:

```
Testing libmd KATS:
panic: pid 2526 (md_kats), uid 0, FIPS error 1: HMAC-SHA1 Known Answer Test: Failed

Testing kernel KATS:
panic: pid 2121 (kernel_kats), uid 0, FIPS error 1: NIST 800-90 HMAC DRBG Known Answer Test:
Failed

Testing Octeon KATS:
panic: pid 2114 (octcrypto_kats), uid 0, FIPS error 1: DES3-CBC Known Answer Test: Failed

Testing JSF Crypto (Octeon) KATs:
panic: pid 2231 (jsf_crypto_octeon_k), uid 0, FIPS error 1: AES-GCM Known Answer Test: Failed

Testing OpenSSL KATS:
panic: pid 2340 (openssl_kats), uid 0, FIPS error 1: NIST 800-90 HMAC DRBG Known Answer Test:
Failed

Testing QuickSec 7.0 KATS:
```

```
panic: pid 37538 (quicksec_7_0_kats), uid 0, FIPS error 1: NIST 800-90 HMAC DRBG Known Answer
Test: Failed
```

RELATED DOCUMENTATION

How to Enable and Configure FIPS Mode in Junos OS | 9

13

CHAPTER

Configuration Statements

checksum-validate

IN THIS SECTION

Syntax

```
checksum-validate {
    match (equal | greater-than | less-than | not-equal);
    value checksum-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol ipv4]
[edit security idp custom-attack attack-name attack-type signature protocol tcp]
[edit security idp custom-attack attack-name attack-type signature protocol udp]
[edit security idp custom-attack attack-name attack-type signature protocol icmp]
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Allow IDP to validate checksum field against the calculated checksum.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value *checksum-value*

Match a decimal value.

- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

code

IN THIS SECTION

Syntax

```
code {
    match (equal | greater-than | less-than | not-equal);
    value code-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the secondary code that identifies the function of the request/reply within a given type.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *code-value*—Match a decimal value.
- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

data-length

IN THIS SECTION

Syntax

```
data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol udp]
[edit security idp custom-attack attack-name attack-type signature protocol icmp]
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
[edit security idp custom-attack attack-name attack-type signature protocol tcp]
```

Description

Specify the number of bytes in the data payload. In the TCP header, for SYN, ACK, and FIN packets, this field should be empty.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`data-length`*—Match the number of bytes in the data payload.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.3.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

destination-option

IN THIS SECTION

Syntax

```
destination-option {
    home-address {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
```

```
    }
    option-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
    }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header]
```

Description

Specify the IPv6 destination option for the extension header. The `destination-option` option inspects the header option type of `home-address` field in the `extension header` and reports a custom attack if a match is found. The `destination-option` supports the `home-address` field type of inspection.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

extension-header

IN THIS SECTION

Syntax

```
extension-header {
    destination-option {
        home-address {
            match (equal | greater-than | less-than | not-equal);
            value header-value;
        }
            option-type {
                match (equal | greater-than | less-than | not-equal);
                value header-value;
            }
    }
    routing-header {
        header-type {
            match (equal | greater-than | less-than | not-equal);
            value header-value;
            }
        }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6]
```

Description

Specify the IPv6 extension header.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

header-type

IN THIS SECTION

Syntax

```
header-type {
    match (equal | greater-than | less-than | not-equal);
    value header-value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-header routing-header]
```

Description

Specify the IPv6 routing header type.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

home-address

IN THIS SECTION

Syntax

```
home-address {
    match (equal | greater-than | less-than | not-equal);
```

```
    value value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header destination-option]
```

Description

Specify the IPv6 home address of the mobile node.

Options

match (equal | greater-than | less-than | not-equal)	Match an operand.
value	Match a decimal value.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

identification

IN THIS SECTION

Syntax

```
identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify a unique value used by the destination system to associate requests and replies.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`identification-value`*—Match a decimal value.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

icmpv6 (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
icmpv6 {
    checksum-validate {
        match (equal | greater-than | less-than | not-equal);
        value checksum-value;
    }
    code {
        match (equal | greater-than | less-than | not-equal);
        value code-value;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    type {
        match (equal | greater-than | less-than | not-equal);
```

```
        value type-value;
    }
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol]
```

Description

Allow IDP to match the attack for the specified ICMPv6.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

ihl (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
ihl {
    match (equal | greater-than | less-than | not-equal);
    value ihl-value;
}
```

Hierarchy Level

```
[edit  set security idp custom-attack ipv4_custom attack-type signature protocol ipv4]
```

Description

Specify the IPv4 header length in words.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 15

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

option-type

IN THIS SECTION

Syntax

```
option-type {
    match (equal | greater-than | less-than | not-equal);
    value header-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header destination-option]
```

Description

Specify the type of option for destination header type.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

reserved (Security IDP Custom Attack)

IN THIS SECTION

Syntax

```
reserved {
    match (equal | greater-than | less-than | not-equal);
```

```
    value reserved-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack ipv4_custom attack-type signature protocol tcp]
```

Description

Specify the three reserved bits in the TCP header field.

Options

match (equal | greater-than | less-than | not-equal)

Match an operand.

value

Match a decimal value.

- **Range:** 0 through 7

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

routing-header

IN THIS SECTION

Syntax

```
routing-header {
    header-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
    }
}
```

Hierarchy Level

```
[edit  set security idp custom-attack attack-name attack-type signature protocol ipv6 extension-
header]
```

Description

Specify the IPv6 routing header type. The `routing-header` option inspects the routing-header type field and reports a custom attack if a match with the specified value is found. The `routing-header` option supports the following routing header types: `routing-header-type0`, `routing-header-type1`, and so on.

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

sequence-number (Security IDP ICMPv6 Headers)

IN THIS SECTION

Syntax

```
sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

Options

- `match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.
- `value` *`sequence-number`*—Match a decimal value.
- **Range:** 0 through 65,535

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104

type (Security IDP ICMPv6 Headers)

IN THIS SECTION

Syntax

```
type {
    match (equal | greater-than | less-than | not-equal);
    value type-value;
}
```

Hierarchy Level

```
[edit security idp custom-attack attack-name attack-type signature protocol icmpv6]
```

Description

Specify the primary code that identifies the function of the request/reply.

Options

`match` (`equal` | `greater-than` | `less-than` | `not-equal`)—Match an operand.

`value` *`type-value`*—Match a decimal value.

- **Range:** 0 through 255

Required Privilege Level

security—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

RELATED DOCUMENTATION

IDP Extended Package Configuration Overview | 104