

Junos[®] OS

Common Criteria Guide for SRX345 and SRX380 Devices

Published
2023-01-22

Release
20.4R1

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos[®] OS Common Criteria Guide for SRX345 and SRX380 Devices

20.4R1

Copyright © 2023 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <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 the Documentation | ix

Documentation and Release Notes | ix

Documentation Conventions | ix

Documentation Feedback | xii

Requesting Technical Support | xii

Self-Help Online Tools and Resources | xiii

Creating a Service Request with JTAC | xiii

1

Overview

Understanding the Common Criteria Evaluated Configuration | 15

Understanding Common Criteria | 15

Supported Platforms | 15

Understanding Junos OS in FIPS Mode of Operation | 16

About the Cryptographic Boundary on Your Device | 17

How FIPS Mode of Operation Differs from Non-FIPS Mode of Operation | 17

Validated Version of Junos OS in FIPS Mode of Operation | 18

Understanding FIPS Mode of Operation Terminology and Supported Cryptographic Algorithms | 18

FIPS Terminology | 18

Supported Cryptographic Algorithms | 20

Identifying Secure Product Delivery | 21

Applying Tamper-Evident Seals to the Cryptographic Module | 22

General Tamper-Evident Seal Instructions | 23

Applying Tamper-Evident Seals on SRX345 Devices | 23

Applying Tamper-Evident Seals on SRX380 Devices | 23

Understanding Management Interfaces | 24

2

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode of Operation | 26

Security Administrator Role and Responsibilities | 26

FIPS User Role and Responsibilities | 27

What Is Expected of All FIPS Users | 28

Understanding Services for Junos OS in FIPS Mode of Operation | 28

Understanding Authenticated Services | 29

Critical Security Parameters | 30

Downloading Software Packages from Juniper Networks | 32

Installing Junos Software Packages | 32

Understanding Zeroization to Clear System Data for FIPS Mode of Operation | 33

Why Zeroize? | 34

When to Zeroize? | 34

Loading Firmware on the Device | 35

How to Enable and Configure Junos OS in FIPS Mode of Operation | 35

3

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Authorized Administrator | 38

Configuring a Network Device Protection Profile Authorized Administrator | 40

4

Configuring SSH and Console Connection

Understanding FIPS Authentication Methods | 43

Username and Password Authentication over the Console and SSH | 43

Username and Public Key Authentication over SSH | 43

Configuring a System Login Message and Announcement | 44

Limiting the Number of User Login Attempts for SSH Sessions | 45

Configuring SSH on the Evaluated Configuration | 47

Configuring SSH Rekey | 48

5

Configuring the Remote Syslog Server

Sample Syslog Server Configuration on a Linux System | 50

- Configuring Event Logging to a Local File | 50

- Configuring Event Logging to a Remote Server | 51

- Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server | 51

Forwarding Logs to the External Syslog Server | 57

6

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration | 60

- Configuring Audit Log Options for SRX345 and SRX380 Devices | 60

Sample Code Audits of Configuration Changes | 61

7

Configuring Event Logging

Event Logging Overview | 65

Interpreting Event Messages | 82

Logging Changes to Secret Data | 83

Login and Logout Events Using SSH | 85

Logging of Audit Startup | 86

8

Configuring a Secure Logging Channel

Creating a Secure Logging Channel | 88

- Configuring a Trusted Path or Channel Between a Device Running Junos OS and a Remote External Storage Server | 89

9

Configuring VPNs

Configuring VPN on a Device Running Junos OS | 96

- Configuring an IPsec VPN with a Preshared Key for IKE Authentication | 98

- Configuring IPsec VPN with Preshared Key as IKE Authentication on the Initiator | 99

- Configuring IPsec VPN with Preshared Key as IKE Authentication on the Responder | 101

- Configuring an IPsec VPN with an RSA Signature for IKE Authentication | 104

- Configuring IPsec VPN with RSA Signature as IKE Authentication on the Initiator or Responder | 105

Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication | 108

Configuring IPsec VPN with ECDSA signature IKE authentication on the Initiator | 109

Configuring IPsec VPN with ECDSA signature IKE authentication on the Responder | 112

10

Configuring Security Flow Policies

Understanding a Security Flow Policy on a Device Running Junos OS | 116

Configuring a Security Flow Policy in Firewall Bypass Mode | 116

Configuring a Security Policy in Firewall Discard Mode | 117

Configuring a Security Flow Policy in IPsec Protect Mode | 117

11

Configuring Traffic Filtering Rules

Overview | 120

Understanding Protocol Support | 120

Configuring Traffic Filter Rules | 122

Configuring Default Deny-All and Reject Rules | 123

Logging the Dropped Packets Using Default Deny-all Option | 124

Configuring Mandatory Reject Rules for Invalid Fragments and Fragmented IP Packets | 125

Configuring Default Reject Rules for Source Address Spoofing | 126

Configuring Default Reject Rules with IP Options | 126

12

Configuring Network Attacks

Configuring IP Teardrop Attack Screen | 130

Configuring TCP Land Attack Screen | 131

Configuring ICMP Fragment Screen | 133

Configuring Ping-Of-Death Attack Screen | 134

Configuring tcp-no-flag Attack Screen | 136

Configuring TCP SYN-FIN Attack Screen | 138

Configuring TCP fin-no-ack Attack Screen | 139

Configuring UDP Bomb Attack Screen | 141

Configuring UDP CHARGEN DoS Attack Screen | 141

Configuring TCP SYN and RST Attack Screen | 143

Configuring ICMP Flood Attack Screen | 145

Configuring TCP SYN Flood Attack Screen | 147

Configuring TCP Port Scan Attack Screen | 148

Configuring UDP Port Scan Attack Screen | 150

Configuring IP Sweep Attack Screen | 152

13

Configuring the IDP Extended Package

IDP Extended Package Configuration Overview | 155

14

Configuring Clustering Mode

Understanding Cluster Mode | 157

Configuring L2 HA Link Encryption tunnel | 157

Configuring PKI based L2 HA Link Encryption tunnel | 163

15

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 173

Performing Power-On Self-Tests on the Device | 173

16

Configuration Statements

checksum-validate | 180

Sample Code Audits of Configuration Changes | 181

data-length | 184

destination-option | 185

extension-header | 186

header-type | 187

home-address | 188

identification | 189

icmpv6 (Security IDP Custom Attack) | 190

ihl (Security IDP Custom Attack) | 191

option-type | 192

reserved (Security IDP Custom Attack) | 193

routing-header | 194

sequence-number (Security IDP ICMPv6 Headers) | 195

type (Security IDP ICMPv6 Headers) | 196

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | ix
- Documentation Conventions | ix
- Documentation Feedback | xii
- Requesting Technical Support | xii

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.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Overview

Understanding the Common Criteria Evaluated Configuration | **15**

Understanding Junos OS in FIPS Mode of Operation | **16**

Understanding FIPS Mode of Operation Terminology and Supported Cryptographic Algorithms | **18**

Identifying Secure Product Delivery | **21**

Applying Tamper-Evident Seals to the Cryptographic Module | **22**

Understanding Management Interfaces | **24**

Understanding the Common Criteria Evaluated Configuration

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. The following list describes the standards to which the device has been evaluated:

- Collaborative Protection Profile for Network Devices, version 2.1, 24 September 2018 (NDcPPv2.1)
- Collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 1.0, 27 February 2015 (FWcPP)
- Collaborative Protection Profile for Network Devices or Collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15 June 2017 (IPSEP)
- Network Device Collaborative Protection Profile (NDcPPv2.1)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, 8 March 2017 (VPNEP)

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:

- The IPSEP, NDcPPv2.1, FWcPP, and VPNEP apply to:
 - SRX345 devices.
 - SRX380 devices.

RELATED DOCUMENTATION

| [Identifying Secure Product Delivery | 21](#)

Understanding Junos OS in FIPS Mode of Operation

IN THIS SECTION

- [About the Cryptographic Boundary on Your Device | 17](#)
- [How FIPS Mode of Operation Differs from Non-FIPS Mode of Operation | 17](#)
- [Validated Version of Junos OS in FIPS Mode of Operation | 18](#)

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. Junos-FIPS is a version of the Junos operating system (Junos OS) that complies with Federal Information Processing Standard (FIPS) 140-2.

Operating SRX Series devices in a FIPS 140-2 Level 2 environment requires enabling and configuring FIPS mode of operation on the device from the Junos OS command-line interface (CLI).

The *Security Administrator* enables FIPS mode of operation in Junos OS Release 20.4R1 and sets up keys and passwords for the system and other *FIPS users* who can view the configuration. Both user types can also perform normal configuration tasks on the device (such as modify interface types) as individual user configuration allows.

BEST PRACTICE: Be sure to verify the secure delivery of your device and apply tamper-evident seals to its vulnerable ports.

About the Cryptographic Boundary on Your Device

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos OS in FIPS mode of operation prevents the cryptographic module from running any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.



CAUTION: Virtual Chassis features are not supported in FIPS mode of operation. Do not configure a Virtual Chassis in FIPS mode of operation.

To physically secure the cryptographic module, all Juniper Networks devices require a tamper-evident seal on the USB and mini-USB ports.

How FIPS Mode of Operation Differs from Non-FIPS Mode of Operation

Unlike Junos OS in non-FIPS mode of operation, Junos OS in FIPS mode of operation is a *nonmodifiable operational environment*. In addition, Junos OS in FIPS mode of operation differs in the following ways from Junos OS in non-FIPS mode of operation:

- Self-tests of all cryptographic algorithms are performed at startup in both FIPS mode and non FIPS mode. But the results are displayed on console only in FIPS mode.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and MD5 are disabled.
- FIPS Mode uses the HMAC-DRBG Random Number Generator, while Non-FIPS mode uses the Junos default yarrow Random Number Generator.
- Pairwise consistency test when a module generates a public and private key pair is performed only in FIPS Mode.
- DH and ECDH public key validation during generation is performed only in FIPS Mode
- Weak or unencrypted management connections must not be configured
- Junos-FIPS administrator passwords must be at least 10 characters long.
- Cryptographic keys must be encrypted before transmission.

The FIPS 140-2 standard is available for download from the National Institute of Standards and Technology (NIST) at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

Validated Version of Junos OS in FIPS Mode of Operation

To determine whether a Junos OS release is NIST-validated, see the compliance page on the Juniper Networks Web site (<https://apps.juniper.net/compliance>).

RELATED DOCUMENTATION

| [Identifying Secure Product Delivery](#) | 21

Understanding FIPS Mode of Operation Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- [FIPS Terminology](#) | 18
- [Supported Cryptographic Algorithms](#) | 20

Use the definitions of FIPS terms and supported algorithms to help you understand Junos OS in FIPS mode of operation.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects.

Cryptographic module—The set of hardware, software, and firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. SRX Series devices are certified at FIPS 140-2 Level 2.

Security Administrator—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode of operation on a device. For details, see *Understanding Roles and Services for Junos OS in FIPS Mode of Operation*.

ESP—Encapsulating Security Payload (ESP) protocol. The part of the IPsec protocol that guarantees the confidentiality of packets through encryption. The protocol ensures that if an ESP packet is successfully decrypted, and no other party knows the secret key the peers share, the packet was not wiretapped in transit.

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos OS in FIPS mode of operation complies with FIPS 140-2 Level 2.

IKE—The Internet Key Exchange (IKE) is part of IPsec and provides ways to securely negotiate the shared private keys that the authentication header (AH) and ESP portions of IPsec need to function properly. IKE employs Diffie-Hellman key-exchange methods and is optional in IPsec. (The shared keys can be entered manually at the endpoints.)

IPsec—The IP Security (IPsec) protocol. A standard way to add security to Internet communications. An IPsec security association (SA) establishes secure communication with another FIPS cryptographic module by means of mutual authentication and encryption.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see *Understanding FIPS Self-Tests*.

SA—Security association (SA). A connection between hosts that allows them to communicate securely by defining, for example, how they exchange private keys. As Security Administrator, you must manually configure an internal SA on devices running Junos OS in FIPS mode of operation. All values, including the keys, must be statically specified in the configuration.

SPI—Security parameter index (SPI). A numeric identifier used with the destination address and security protocol in IPsec to identify an SA. Because you manually configure the SA for Junos OS in FIPS mode of operation, the SPI must be entered as a parameter rather than derived randomly.

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and **rcp** in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos OS, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Zeroization—Erasure of all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module—or in preparation for repurposing the device for non-FIPS operation. The Security Administrator can zeroize the system with a CLI operational command. For details, see *Understanding Zeroization to Clear System Data for FIPS Mode of Operation*.

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

BEST PRACTICE: For FIPS 140-2 compliance, use only FIPS-approved cryptographic algorithms in Junos OS in FIPS mode of operation.

The following cryptographic algorithms are supported in FIPS mode of operation. Symmetric methods use the same key for encryption and decryption, while asymmetric methods (preferred) use different keys for encryption and decryption.

AES—The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method, and keys are typically used only for a short time, discarded, and regenerated.

ECDH—Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA using the P-256, P-384, or the P-521 curve can be configured under OpenSSH.

HMAC—Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos OS in FIPS mode of operation, HMAC uses the iterated cryptographic hash function SHA-1 (designated as HMAC-SHA1) along with a secret key.

3DES (3des-cbc)—Encryption standard based on the original Data Encryption Standard (DES) from the 1970s that used a 56-bit key and was cracked in 1997. The more secure 3DES is DES enhanced with three multiple stages and effective key lengths of about 112 bits. For Junos OS in FIPS mode of operation, 3DES is implemented with cipher block chaining (CBC).

RELATED DOCUMENTATION

Understanding Zeroization to Clear System Data for FIPS Mode of Operation

Understanding FIPS Self-Tests

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](#) | 15

Applying Tamper-Evident Seals to the Cryptographic Module

IN THIS SECTION

- [General Tamper-Evident Seal Instructions](#) | 23

The cryptographic module physical embodiment is that of a multi-chip standalone device that meets Level 2 physical security requirements. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel, and brushed aluminum enclosure. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow for any sort of observation of any component contained within the cryptographic boundary. Tamper-evident seals allow the operator to verify if the enclosure has been breached. These seals are not factory-installed and must be applied by the Cryptographic Officer.

NOTE: Seals are available for order from Juniper Networks using part number JNPR-FIPS-TAMPER-LBLS.

As a Cryptographic Officer, you are responsible for:

- Applying seals to secure the cryptographic module

- Controlling any unused seals
- Controlling and observing any changes, such as repairs or booting from an external USB drive to the cryptographic module, that require removing or replacing the seals to maintain the security of the module

As per the security inspection guidelines, upon receipt of the cryptographic module, the Cryptographic Officer must check that the labels are free of any tamper evidence.

General Tamper-Evident Seal Instructions

All FIPS-certified switches require a tamper-evident seal on the USB port. While applying seals, follow these general instructions:

- Handle the seals with care. Do not touch the adhesive side. Do not cut or otherwise resize a seal to make it fit.
- Make sure all surfaces to which the seals are applied are clean and dry and clear of any residue.
- Apply the seals with firm pressure across the seal to ensure adhesion. Allow at least 24 hours for the adhesive to cure.

Applying Tamper-Evident Seals on SRX345 Devices

On SRX345 devices, apply 27 tamper-evident seals at the following locations:

1. Apply five seals at the top of the chassis, covering one of the five chassis screws.
2. Apply four seals on the I/O slots.
3. Apply two seals on the rear panel, covering the blank faceplate and the SSD.
4. Apply 16 seals, on the side panels over the screw holes.

Applying Tamper-Evident Seals on SRX380 Devices

On SRX380 devices, apply tamper-evident seals at the following locations:

1. Apply four seals on the front I/O slots.
2. Apply five seals at the top of the chassis, covering one of the five chassis screws.
3. Apply two seals at the front of the chassis on either side of the LED matrix on the right of the device.
4. Apply two seals on the rear panel, covering the blank faceplate. If the grounding connection is not used, apply a seal across this as well.

RELATED DOCUMENTATION

| [How to Enable and Configure Junos OS in FIPS Mode of Operation](#) | 35

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.

RELATED DOCUMENTATION

| [Understanding the Common Criteria Evaluated Configuration](#) | 15

2

CHAPTER

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode of Operation | 26

Understanding Services for Junos OS in FIPS Mode of Operation | 28

Downloading Software Packages from Juniper Networks | 32

Installing Junos Software Packages | 32

Understanding Zeroization to Clear System Data for FIPS Mode of Operation | 33

Loading Firmware on the Device | 35

How to Enable and Configure Junos OS in FIPS Mode of Operation | 35

Understanding Roles and Services for Junos OS in FIPS Mode of Operation

IN THIS SECTION

- [Security Administrator Role and Responsibilities | 26](#)
- [FIPS User Role and Responsibilities | 27](#)
- [What Is Expected of All FIPS Users | 28](#)

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode of operation allows a wide range of capabilities for users, and authentication is identity-based. In contrast, the FIPS 140-2 standard defines two user roles: *Security Administrator* and *FIPS user*. These roles are defined in terms of Junos OS user capabilities.

All other user types defined for Junos OS in FIPS mode of operation (operator, administrative user, and so on) must fall into one of the two categories: Security Administrator or FIPS user. For this reason, user authentication in FIPS mode of operation is role-based.

In addition to their FIPS roles, both user types can perform normal configuration tasks on the device as individual user configuration allows.

Security Administrators and FIPS users perform all FIPS-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode of operation. Security Administrator and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode of operation.

For details, see:

Security Administrator Role and Responsibilities

The Security Administrator is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode of operation on a device. The Security Administrator 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 Security Administrator can configure and monitor the module through a console or SSH connection.

BEST PRACTICE: We recommend that the Security Administrator administer the system in a secure manner by keeping passwords secure and checking audit files.

The permissions that distinguish the Security Administrator from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the Security Administrator to a login class that contains all of these permissions. A user with the Junos OS maintenance permission can read files containing critical security parameters (CSPs).

NOTE: Junos OS in FIPS mode of operation does not support the *FIPS 140-2 maintenance role*, which is different from the Junos OS maintenance permission.

Among the tasks related to Junos OS in FIPS mode of operation, the Security Administrator is expected to:

- Set the initial root password.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Set up manual IPsec SAs for configuration with dual Routing Engines.
- Examine log and audit files for events of interest.
- Erase user-generated files and data on (zeroize) the device.

FIPS User Role and Responsibilities

All FIPS users, including the Security Administrator, can view the configuration. Only the user assigned as the Security Administrator can modify the configuration.

The permissions that distinguish Security Administrators from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the FIPS user to a class that contains *none* of these permissions.

FIPS users configure networking features on the device and perform other tasks that are not specific to FIPS mode of operation. FIPS users who are not Security Administrators can perform reboots and view status output.

What Is Expected of All FIPS Users

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

All FIPS users must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
 - Users are trusted.
 - Users abide by all security guidelines.
 - Users do not deliberately compromise security.
 - Users behave responsibly at all times.

RELATED DOCUMENTATION

[Understanding Zeroization to Clear System Data for FIPS Mode of Operation](#) | 33

Understanding Services for Junos OS in FIPS Mode of Operation

IN THIS SECTION

- [Understanding Authenticated Services](#) | 29
- [Critical Security Parameters](#) | 30

All services implemented by the module are listed in the tables that follow.

Understanding Authenticated Services

Table 3 on page 29 lists the authenticated services on the device running Junos OS.

Table 3: Authenticated services

Authenticated Services	Description	Security Administrator	User (read-only)	User (network)
Configure security	Security relevant configuration	x	–	–
Configure	Non-security relevant configuration	x	–	–
Secure traffic	IPsec protected routing	–	–	x
Status	Display the status	x	x	–
Zeroize	Destroy all critical security parameters (CSPs)	x	–	–
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x	–
IPsec connect	Initiate IPsec connection (IKE)	x	–	x
Console access	Console monitoring and control (CLI)	x	x	–
Remote reset	Software-initiated reset	x	–	–

Table 4: Unauthenticated traffic

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services

Critical Security Parameters

Critical security parameters (CSPs) are security-related information such as cryptographic keys and passwords that can compromise the security of the cryptographic module or the security of the information protected by the module if they are disclosed or modified.

Zeroization of the system erases all traces of CSPs in preparation for operating the device as a cryptographic module.

[Table 5 on page 30](#) lists the CSP access rights within services.

Table 5: CSP Access Rights Within Services

Service	CSPs					
	DRBG_Seed	DRBG_State	SSH PHK	SSH DH	SSH-SEK	ESP-SEK
Configure security	-	E	G, W	-	-	-
Configure	-	-	-	-	-	-
Secure Traffic	-	-	-	-	-	E
Status	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z
SSH connect	-	E	E	G, E	G, E	-
IPSec connect	-	E	-	-	-	G
Console access	-	-	-	-	-	-
Remote reset	G, E	G	-	Z	Z	Z
Local Reset	G, E	G	-	Z	Z	Z
Traffic	-	-	-	-	-	-

Service	CSPs				
	IKE-PSK	IKE-Priv	IKE-SKEYI	IKE-SKE	IKE-DH-PRI
Configure security	W	G, W	-	-	-

Service	CSPs				
	IKE-PSK	IKE-Priv	IKE-SKEYI	IKE-SKE	IKE-DH-PRI
Configure	-	-	-	-	-
Secure Traffic	-	-	-	E	-
Status	-	-	-	-	-
Zeroize	Z	Z	-	-	-
SSH connect	-	-	-	-	-
IPSec connect	E	E	G	G	G
Console access	-	-	-	-	-
Remote reset	-	-	Z	Z	Z
Local Reset	-	-	Z	Z	Z
Traffic	-	-	-	-	-

Here:

- G = Generate: The device generates the CSP.
- E = Execute: The device runs using the CSP.
- W = Write: The CSP is updated or written to the device.
- Z = Zeroize: The device zeroizes the CSP.

RELATED DOCUMENTATION

[Understanding Zeroization to Clear System Data for FIPS Mode of Operation | 33](#)

[Understanding FIPS Authentication Methods | 43](#)

Downloading Software Packages from Juniper Networks

To operate in Junos OS in FIPS mode, the device must have the following software packages installed. You can download the following Junos OS software package 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

SRX Series devices can provide the security defined by Federal Information Processing Standards (FIPS) 140-2 Level 2 if these devices are operated in the Junos OS 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 and the Junos FIPS mode package from <https://support.juniper.net/support/downloads/>. See [Downloading Software](#).
2. Install the Junos OS on your device using a TFTP server, see [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server](#) or 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 to Clear System Data for FIPS Mode of Operation

IN THIS SECTION

- [Why Zeroize? | 34](#)
- [When to Zeroize? | 34](#)

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 FIPS mode you need to zeroize the device.

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 Security Administrator must zeroize the non-approved mode critical security parameters (CSPs). For SRX345 and SRX380 devices, the Security Administrator 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 Security Administrator.



CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the device. This command erases all the CSPs, configurations, and the hard disk partitions containing the device image. Hence, the device does not boot up on zeroization and USB reimage is required to recover the device.

Zeroization can be time-consuming. Although all configurations are removed in a few seconds, the zeroization process goes on to overwrite all media, which can take considerable time depending on the size of the media.

Why Zeroize?

Your device is not considered a valid FIPS cryptographic module until all CSPs have been entered—or reentered—while the device is in FIPS mode of operation.

BEST PRACTICE: For FIPS 140-2 compliance, we recommend that you zeroize the device to exit the FIPS mode.

When to Zeroize?

As a Security Administrator, perform zeroization in the following situations:

- **Before FIPS operation**—To prepare your device for operation as a FIPS cryptographic module, perform zeroization to remove the non-approved mode critical security parameters (CSPs) and enable FIPS mode on the device.
- **Before non-FIPS operation**—To begin repurposing your device for non-FIPS operation, perform zeroization on the device.

NOTE: Juniper Networks does not support installing non-FIPS software in a FIPS mode of operation, but doing so might be necessary in certain test environments. Be sure to zeroize the system first.

- **When a tamper-evident seal is disturbed**—If the seal on an insecure port has been tampered with, the system is considered to be compromised. After applying new tamper-evident seals to the appropriate locations, zeroize the system and set up new passwords and CSPs.

RELATED DOCUMENTATION

| [Applying Tamper-Evident Seals to the Cryptographic Module](#) | 22

Loading Firmware on the Device

The Junos OS 20.4R1 images only accept the firmware signed with ECDSA and rejects any firmware signed with RSA+SHA1. You cannot downgrade to images that are signed with RSA+SHA1 from "ECDSA signed only" images. In this scenario, the SRX Series device does not load the firmware.

RELATED DOCUMENTATION

| [How to Enable and Configure Junos OS in FIPS Mode of Operation](#)

How to Enable and Configure Junos OS in FIPS Mode of Operation

You, as Cryptographic Officer, can enable and configure Junos OS in FIPS mode of operation on your device. Before you begin enabling and configuring FIPS mode of operation on the device:

- Verify the secure delivery of your device. See [“Identifying Secure Product Delivery” on page 21](#).
- [Applying Tamper-Evident Seals to the Cryptographic Module on page 22](#)

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

1. Zeroize the device before enabling FIPS mode of operation

```
user@host> request system zeroize
```

2. Delete the web management services.

```
user@host# delete system services web-management https
```

3. Enable the FIPS mode on the device.

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

4. Set the root password.

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

```
New password: type password here
```

```
Retype new password: retype password here
```

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

```
user@host# commit
```

6. 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 [20.4R1]
```

RELATED DOCUMENTATION

| [Loading Firmware on the Device](#) | 35

3

CHAPTER

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Authorized Administrator | 38

Configuring a Network Device Protection Profile Authorized Administrator | 40

Understanding the Associated Password Rules for an Authorized Administrator

The authorized administrator 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 FIPS 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

[Understanding Junos OS in FIPS Mode of Operation | 16](#)

[Identifying Secure Product Delivery | 21](#)

Configuring a Network Device Protection Profile Authorized Administrator

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.

An NDPP 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 NDPP user authorized administrator.

```
[edit]  
root@host# set system login user NDcPPv2-user class security-admin authentication encrypted-password
```

OR

```
[edit]  
root@host# set system login user NDcPPv2-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 Authorized Administrator](#) | 38

4

CHAPTER

Configuring SSH and Console Connection

Understanding FIPS Authentication Methods | 43

Configuring a System Login Message and Announcement | 44

Limiting the Number of User Login Attempts for SSH Sessions | 45

Configuring SSH on the Evaluated Configuration | 47

Configuring SSH Rekey | 48

Understanding FIPS Authentication Methods

The Juniper Networks Junos operating system (Junos OS) running in FIPS 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 FIPS mode of operation:

- [Username and Password Authentication over the Console and SSH on page 43](#)
- [Username and Public Key Authentication over SSH on page 43](#)

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 $5.6e7/(2^{128})$.

NOTE: The ssh-rsa authentication method is one of the allowed algorithms in FIPS mode.

RELATED DOCUMENTATION

| [Configuring SSH on the Evaluated Configuration](#) | 47

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](#) | 47

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 3 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](#) | 47

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.

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 [ dh-group14-sha1 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-sha1 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 ]
```

RELATED DOCUMENTATION

[Understanding FIPS Authentication Methods | 43](#)[Limiting the Number of User Login Attempts for SSH Sessions | 45](#)

Configuring SSH Rekey

The SSHv2 protocol provides secure terminal sessions utilizing the secure encryption. The SSHv2 protocol enforces running the key-exchange phase and changing the encryption and integrity keys for the session. Key exchange is done periodically, after specified seconds or after specified bytes of data have passed over the connection. You can configure thresholds for SSH rekeying (FCS_SSHS_EXT.1.8 and FCS_SSHC_EXT.1.8). The TSF ensures that within the SSH connections the same session keys are used for a threshold for an hour, and less than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.

To configure SSH rekey on the TOE:

1. Specify the data-limit.

```
[edit system services ssh rekey]
user@host# set data-limit data-limit [51200..4294967295 bytes]
```

2. Specify the time-limit.

```
[edit system services ssh rekey]
user@host# set time-limit time-limit [1..1440 minutes]
```

RELATED DOCUMENTATION

[Understanding FIPS Authentication Methods | 43](#)[Limiting the Number of User Login Attempts for SSH Sessions | 45](#)

5

CHAPTER

Configuring the Remote Syslog Server

Sample Syslog Server Configuration on a Linux System | **50**

Forwarding Logs to the External Syslog Server | **57**

Sample Syslog Server Configuration on a Linux System

IN THIS SECTION

- [Configuring Event Logging to a Local File | 50](#)
- [Configuring Event Logging to a Remote Server | 51](#)
- [Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server | 51](#)

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 NDcPP 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@NDcPP_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
AAAAB3NzaClyc2EAAAADAQABAAQCrUREJUBpjwAoIgRrGy9zgt+
D2pikk3Q/Wdf8I5vr+njeqJhCx2bUAkrRbYXNILQQAZbg7kLfi/8TqqL
eon4HOP2e6oCSorKdx/GrOTzLONL4fh0EyuSAk8bs5JuwWNBUokV025
gzpGFsBusGnlj6wqqJ/sjFsMmfxYCbY+pUWb8m1/A9YjOFT+6esw+9S
tF6Gbg+VpbYYk/Oday4z+z7tQHRFSrxj2G92aoliVDBLJpareEMBc8w
LdSUDxmgBTM2oadOmm+kreBUQjrMr6775RJn9H9YwIxKOxGm4SFnX/Vl4
R+lZ9RqmKH2wodIEM34K0wXEHZAzNZ0loLmaAVqT
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 access 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 access 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

6

CHAPTER

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration | **60**

Sample Code Audits of Configuration Changes | **61**

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

- [Configuring Audit Log Options for SRX345 and SRX380 Devices | 60](#)

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

Configuring Audit Log Options for SRX345 and SRX380 Devices

To configure audit log options for SRX345 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](#) | 61

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*

7

CHAPTER

Configuring Event Logging

Event Logging Overview | **65**

Interpreting Event Messages | **82**

Logging Changes to Secret Data | **83**

Login and Logout Events Using SSH | **85**

Logging of Audit Startup | **86**

Event Logging Overview

The evaluated configuration requires the auditing of configuration changes through the system log.

In addition, Junos OS can:

- Send automated responses to audit events (syslog entry creation).
- Allow authorized managers to examine audit logs.
- Send audit files to external servers.
- Allow authorized managers to return the system to a known state.

The logging for the evaluated configuration must capture the events. The logging events are listed below:

[Table 6 on page 65](#) shows sample for syslog auditing for NDcPPv2:

Table 6: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FAU_GEN.1	None	None	
FAU_GEN.2	None	None	
FAU_STG_EXT.1	None	None	
FAU_STG.1	None	None	
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/ DataEncryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	
FCS_RBG_EXT.1	None	None	

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FDP_RIP.2	None	None	
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	sshd - SSHD_LOGIN_ATTEMPTS_THRESHOLD [junos@2636.1.1.1.2.164 limit="3" username="root"] Threshold for unsuccessful authentication attempts (3) reached by user 'root'
FIA_PMG_EXT.1	None	None	

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			<p>Successful Remote Login</p> <p>mgd 70652 UI_AUTH_EVENT [junos@2636.1.1.1.2.164 username="root" authentication-level="super-user"] Authenticated user 'root' assigned to class 'super-user'</p> <p>mgd 70652 UI_LOGIN_EVENT [junos@2636.1.1.1.2.164 username="root" class-name="super-user" local-peer="" pid="70652" ssh-connection="10.223.5.251 53476 10.204.134.54 22" client-mode="cli"] User 'root' login, class 'super-user' [70652], ssh-connection '10.223.5.251 53476 10.204.134.54 22', client-mode 'cli'</p> <p>Unsuccessful Remote Login</p> <p>sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="10.223.5.251"] Login failed for user 'root' from host '10.223.5.251'</p> <p>Successful Local Login</p> <p>login 2671 LOGIN_INFORMATION [junos@2636.1.1.1.2.164 username="root" hostname="[unknown\]" tty-name="ttyu0"] User root logged in from host [unknown] on device ttyu0</p> <p>login 2671 LOGIN_ROOT [junos@2636.1.1.1.2.164 username="root" hostname="[unknown\]" tty-name="ttyu0"] User root logged in as root from host [unknown] on device ttyu0</p> <p>Unsuccessful Local Login</p> <p>login 70818 LOGIN_PAM_ERROR [junos@2636.1.1.1.2.164 username="root" error-message="error in service module"] Failure while authenticating user root: error in</p>

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			service module login 70818 LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="ttyu0"] Login failed for user root from host ttyu0

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			<p>Successful Remote Login</p> <p>mgd 70652 UI_AUTH_EVENT [junos@2636.1.1.1.2.164 username="root" authentication-level="super-user"] Authenticated user 'root' assigned to class 'super-user'</p> <p>mgd 70652 UI_LOGIN_EVENT [junos@2636.1.1.1.2.164 username="root" class-name="super-user" local-peer="" pid="70652" ssh-connection="10.223.5.251 53476 10.204.134.54 22" client-mode="cli"] User 'root' login, class 'super-user' [70652], ssh-connection '10.223.5.251 53476 10.204.134.54 22', client-mode 'cli'</p> <p>Unsuccessful Remote Login</p> <p>sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="10.223.5.251"] Login failed for user 'root' from host '10.223.5.251'</p> <p>Successful Local Login</p> <p>login 2671 LOGIN_INFORMATION [junos@2636.1.1.1.2.164 username="root" hostname="[unknown\]" tty-name="ttyu0"] User root logged in from host [unknown] on device ttyu0</p> <p>login 2671 LOGIN_ROOT [junos@2636.1.1.1.2.164 username="root" hostname="[unknown\]" tty-name="ttyu0"] User root logged in as root from host [unknown] on device ttyu0</p> <p>Unsuccessful Local Login</p> <p>login 70818 LOGIN_PAM_ERROR [junos@2636.1.1.1.2.164 username="root" error-message="error in service module"] Failure while authenticating user root: error in</p>

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			<p>service module</p> <p>login 70818 LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="ttyu0"] Login failed for user root from host ttyu0</p>
FIA_UAU.7	None	None	
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	None	<p>UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.164 username="sec-officer" command="request system software add /var/tmp/junos-srxsme-20.4R1.1.tgz no-validate "] User 'sec-officer', command 'request system software add /var/tmp/junos-srxsme-20.4R1.1.tgz no-validate '</p>
FMT_MTD.1/CoreData	All management activities of TSF data	None	Refer to the audit events listed in this table.
FMT_SMF.1/IPS	None	None	None
FMT_SMF.1/ND	None	None	None
FMT_SMF.1/FFW	All management activities of TSF data (including creation, modification and deletion of firewall rules).	None	<p><30>1 2020-08-11T11:15:00.025-07:00 cartier nsd 2095 NSD_SYS_TIME_CHANGE - System time has changed. <38>1 2020-08-11T11:15:25.214-07:00 cartier init - - chassis-control (PID 2059) exited with status=69 <38>1 2020-08-11T11:15:25.217-07:00 cartier init - - chassis-control (PID 47908) started <29>1 2020-08-11T11:16:08.805-07:00 cartier chassisd 47908 CHASSISD_RECONNECT_SUCCESSFUL - Successfully reconnected on soft restart</p>
FMT_SMR.2	None	None	

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	
FPT_TST_EXT.1	None	None	
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.164 username="sec-officer" command="request system software add /var/tmp/junos-srxsme-20.4R1.1.tgz no-validate "] User 'sec-officer', command 'request system software add /var/tmp/junos-srxsme-20.4R1.1.tgz no-validate '
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed through an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (such as, IP address).	mgd 71079 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.164 username="root" command="set date 202005201815.00 "] User 'root', command 'set date 202005201815.00 ' mgd 71079 UI_COMMIT_PROGRESS [junos@2636.1.1.1.2.164 message="signaling 'Network security daemon', pid 2641, signal 31, status 0 with notification errors enabled"] Commit operation in progress: signaling 'Network security daemon', pid 2641, signal 31, status 0 with notification errors enabled nsd 2641 NSD_SYS_TIME_CHANGE - System time has changed
FTA_SSL_EXT.1 (if <i>terminate the session</i> is selected)	The termination of a local interactive session by the session locking mechanism.	None	cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.164 username="root"] Idle timeout for user 'root' exceeded and session terminated
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None	cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.164 username="root"] Idle timeout for user 'root' exceeded and session terminated

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FTA_SSL.4	The termination of an interactive session.	None	mgd 71668 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.164 username="root"] User 'root' logout
FTA_TAB.1	None	None	
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	sshd 72404 - - Unable to negotiate with 1.1.1.2 port 42168: no matching cipher found. Their offer: chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr,aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-cbc, aes192-cbc, aes256-cbc
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	Initiation of the trusted path sshd 72418 - - Accepted keyboard-interactive/pam for root from 10.223.5.251 port 42482 ssh2 Termination of the trusted path sshd 72418 - - Disconnected from user root 10.223.5.251 port 42482 Failure of the trusted path sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="10.223.5.251"] Login failed for user 'root' from host '10.223.5.251'

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None	Initiation of the trusted path sshd 72418 - - Accepted keyboard-interactive/pam for root from 10.223.5.251 port 42482 ssh2 Termination of the trusted path sshd 72418 - - Disconnected from user root 10.223.5.251 port 42482 Failure of the trusted path sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.164 username="root" source-address="10.223.5.251"] Login failed for user 'root' from host '10.223.5.251'
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	sshd 72404 - - Unable to negotiate with 1.1.1.2 port 42168: no matching cipher found. Their offer: chacha20-poly1305@openssh.com, aes128-ctr,aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-cbc, aes192-cbc, aes256-cbc
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure	verify-sig 72830 - - cannot validate ecerts.pem: subject issuer mismatch: /C=US/ST=CA/L=Sunnyvale/O=Juniper Networks/OU=Juniper CA/CN=PackageProduction TestEc_2017_NO_DEFECTS/emailAddress =ca@juniper.net
FIA_X509_EXT.2	None	None	
FIA_X509_EXT.3	None	None	

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FMT_MOF.1/Functions	Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full.	None	mgd 71891 UI_RESTART_EVENT [junos@2636.1.1.1.2.164 username="root" process-name="Network security daemon" description=" immediately"] User 'root' restarting daemon 'Network security daemon' immediately init - - network-security (PID 72907) terminated by signal number 9! init - - network-security (PID 72929) started
FMT_MOF.1/Services	Starting and stopping of services.	None	
FMT_MTD.1/ CryptoKeys	Management of cryptographic keys.	None	SSH key ssh-keygen 2706 - - Generated SSH key file /root/.ssh/id_rsa.pub with fingerprint SHA256:EQotXjlahhIVplg + YBLbFR3TdmJMpm6D1FSjRo6IVE4 ssh-keygen 2714 - - Generated SSH key file /root/.ssh/id_ecdsa.pub with fingerprint SHA256:ubQWoesME9bpOT1e/sYv871hwWUzSG8hNqyMUe1cNc0 IPSEC keys pkid 2458 PKID_PV_KEYPAIR_GEN [junos@2636.1.1.1.2.164 argument1="384" argument2="ECDSA" argument3="cert1"] A 384 bit ECDSA key-Pair has been generated for cert1 pkid 2458 PKID_PV_KEYPAIR_GEN [junos@2636.1.1.1.2.164 argument1="4096" argument2="RSA" argument3="cert2"] A 4096 bit RSA key-Pair has been generated for cert2

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses. Source and destination ports. Transport Layer Protocol TOE Interface	RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.164 source-address="1.1.1.2" source-port="10001" destination-address="2.2.2.2" destination-port="21" connection-tag="0" service-name="junos-ftp" nat-source-address="1.1.1.2" nat-source-port="10001" nat-destination-address="2.2.2.2" nat-destination-port="21" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="p1" source-zone-name="ZO_A" destination-zone-name="ZO_B" session-id-32="5" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/0.0" application="UNKN OWN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A"] session created 1.1.1.2/10001->2.2.2.2/21 0x0 junos-ftp 1.1.1.2/10001->2.2.2.2/21 0x0 N/A N/A N/A N/A 6 p1 ZO_A ZO_B 5 N/A(N/A) ge-0/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets. Identifier of rule causing packet drop	

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			RT_FLOW - RT_FLOW_SESSION_DENY [junos@2636.1.1.1.2.164 source-address="1.1.1.2" source-port="10001" destination-address="2.2.2.2" destination-port="21" connection-tag="0" service-name="junos-ftp" protocol-id="6" icmp-type="0" policy-name="p2" source-zone-name="ZO_A" destination-zone-name="ZO_B" application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/0.0" encrypted="No" reason="Denied by policy" session-id-32="3" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A"] session denied 1.1.1.2/10001->2.2.2.2/21 0x0 junos-ftp 6(0) p2 ZO_A ZO_B UNKNOWN UNKNOWN N/A(N/A) ge-0/0/0.0 No Denied by policy 3 N/A N/A -1 N/A N/A N/A
FFW_RUL_EXT.2	None	None	

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment	<p>kmd 6619 KMD_VPN_UP_ALARM_USER [junos@2636.1.1.1.2.164 vpn-name="vpn1" remote-address="5.5.5.1" local-address="11.11.11.1" gateway-name="gw1" group-name="vpn1" tunnel-id="131073" interface-name="st0.0" internal-ip="Not-Available" name="11.11.11.1" peer-name="5.5.5.1" client-name="Not-Applicable" vrrp-group-id="0" traffic-selector-name="" traffic-selector-cfg-local-id="ipv4_subnet(any:0,[0..7])=0.0.0.0/0" traffic-selector-cfg-remote-id="ipv4_subnet(any:0,[0..7])=0.0.0.0/0" argument1="Static"] VPN vpn1 from 5.5.5.1 is up. Local-ip: 11.11.11.1, gateway name: gw1, vpn name: vpn1, tunnel-id: 131073, local tunnel-if: st0.0, remote tunnel-ip: Not-Available, Local IKE-ID: 11.11.11.1, Remote IKE-ID: 5.5.5.1, AAA username: Not-Applicable, VR id: 0, Traffic-selector: , Traffic-selector local ID: ipv4_subnet(any:0,[0..7])=0.0.0.0/0, Traffic-selector remote ID: ipv4_subnet(any:0,[0..7])=0.0.0.0/0, SA Type: Static</p>

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FIA_X509_EXT.1	Session establishment with CA	Entire packet contents of packets transmitted/received during session establishment	kmd 7200 KMD_VPN_UP_ALARM_USER [junos@2636.1.1.1.2.164 vpn-name=""vpn1"" remote-address=""5.5.5.1"" local-address=""11.11.11.1"" ga teway-name=""gw1"" group-name=""vpn1"" tunnel-id=""131073"" interface-name=""st0.0"" internal-ip=""Not-Available"" name=""11.11.11.1"" peer-name=""5.5.5.1"" client-name=""Not-Applicable"" vrrp-group-id=""0"" traffic-selector-name= """" traffic-selector-cfg-local-id=""ipv4_subnet(any:0, [0..7\]=0.0.0.0/0)"" traffic-selector-cfg-remote-id= ""ipv4_subnet(any: 0,[0..7\]=0.0.0.0/0)"" argument1= ""Static""] VPN vpn1 from 5.5.5.1 is up. Local-ip: 11.11.11.1, gateway name: gw1, vpn name: vpn1, tunnel-id: 131073, local tunnel-if: st0.0, remote tunnel-ip: Not-Available, Local IKE-ID: 11.11.11.1, Remote IKE-ID: 5.5.5.1, AAA username: Not-Applicable, VR id: 0, Traffic-selector: , Traffic-selector local ID: ipv4_subnet(any:0,[0..7\]=0.0.0.0/0), Traffic-selector remote ID: ipv4_subnet(any:0,[0..7\]=0.0.0.0/0), SA Type: Static

Table 6: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses. Source and destination ports. Transport Layer Protocol TOE Interface	RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.164 source-address="1.1.1.2" source-port="10001" destination-address="2.2.2.2" destination-port="53" connection-tag="0" service-name="junos-dns-udp" nat-source-address="1.1.1.2" nat-source-port="10001" nat-destination-address="2.2.2.2" nat-destination-port="53" nat-connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="17" policy-name="p1" source-zone-name="A" destination-zone-name="B" session-id-32="1" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/0.0" application="UNKNOWN WN" nested-application="UNKNOWN" encrypted="UNKNOWN" application-category="N/A" application-sub-category="N/A" application-risk="-1" application-characteristics="N/A" src-vrf-grp="N/A" dst-vrf-grp="N/A"] session created 1.1.1.2/10001->2.2.2.2/53 0x0 junos-dns-udp 1.1.1.2/10001->2.2.2.2/53 0x0 N/A N/A N/A N/A 17 p1 A B 1 N/A(N/A) ge-0/0/0.0 UNKNOWN UNKNOWN UN KNOWN N/A N/A -1 N/A N/A N/A
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets	

Table 6: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			<p>""PERF_MON - RTPERF_CPU_UTIL_MAX [junos@2636.1.1.1.2.164 fpc-slot=""0"" pic-slot=""0"""] FPC 0 PIC 0 CPU Utilization greater than 99, expect packet loss""</p> <p>""PERF_MON - RTPERF_CPU_THRESHOLD_EXCEEDED [junos@2636.1.1.1.2.164 fpc-slot=""0"" pic-slot=""0"" current-value=""93"""] FPC 0 PIC 0 CPU utilization exceeds threshold, current value = 93"" ""RT_FLOW - FLOW_RESOURCE_CHANGE [junos@2636.1.1.1.2.164 resource-name=""session table"" reason=""is full"""] Flow resource session table is full""</p>

In addition, Juniper Networks recommends:

- To capture all changes to the configuration.
- To store logging information remotely.

For more information on log details, see [Specifying Log File Size, Number, and Archiving Properties](#)

RELATED DOCUMENTATION

| [Interpreting Event Messages](#)

Interpreting Event Messages

The following output shows a sample event message.

```
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]
```

Table 7 on page 83 describes the fields for an event message. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 7: Fields in Event Messages

Field	Description	Examples
timestamp	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> • MMM-DD HH:MM:SS.MS+/-HH:MM, is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). • YYYY-MM-DDTHH:MM:SS.MSZ is the year, month, day, hour, minute, second and millisecond in UTC. 	Jul 24 17:43:28 is the timestamp expressed as local time in the United States. 2012-07-24T09:17:15.719Z is 9:17 AM UTC on 24 July 2012.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	4153
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
username	Username of the user initiating the event.	"admin"
message-text	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

RELATED DOCUMENTATION

| [Event Logging Overview](#) | 65

Logging Changes to Secret Data

The following are examples of audit logs of events that change the secret data.

Load Merge

When a **load merge** command is issued to merge the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system radius-server 1.2.3.4 secret]
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user admin authentication encrypted-password]
Jul 24 17:43:28  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user admin2 authentication encrypted-password]
```

Load Replace

When a **load replace** command is issued to replace the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace:
[system radius-server 1.2.3.4 secret]
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace:
[system login user admin authentication encrypted-password]
Jul 24 18:29:09  router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace:
[system login user admin authentication encrypted-password]
```

Load Override

When a **load override** command is issued to override the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 25 14:25:51  router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a
'load override'
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' override:
CC_config2.txt
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system radius-server 1.2.3.4 secret]
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user admin authentication encrypted-password]
Jul 25 14:25:51  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user admin authentication encrypted-password]
```

Load Update

When a **load update** command is issued to update the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 25 14:31:03  router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a
'load update'
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' update:
CC_config2.txt
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system radius-server 1.2.3.4 secret]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate:
[system radius-server 1.2.3.4 secret] ""
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user admin authentication encrypted-password]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate:
[system login user admin authentication encrypted-password] ""
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set:
[system login user test authentication encrypted-password]
Jul 25 14:31:03  router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate:
[system login user test authentication encrypted-password] ""
```

RELATED DOCUMENTATION

[Interpreting Event Messages](#) | 82

Login and Logout Events Using SSH

System log messages are generated whenever a user successfully or unsuccessfully attempts SSH access. Logout events are also recorded. For example, the following logs are the result of two failed authentication attempts, then a successful one, and finally a logout:

```
Dec 20 23:17:35  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port
1673 ssh2
Dec 20 23:17:42  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port
1673 ssh2
Dec 20 23:17:53  bilbo sshd[16645]: Accepted password for op from 172.17.58.45
```

```

port 1673 ssh2
Dec 20 23:17:53 bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at
permission level                               'j-operator'
Dec 20 23:17:53 bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class
'j-operator' [16648]
Dec 20 23:17:56 bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit
'
Dec 20 23:17:56 bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout

```

RELATED DOCUMENTATION

[Interpreting Event Messages](#) | 82

Logging of Audit Startup

The audit information logged includes startups of Junos OS. This in turn identifies the startup events of the audit system, which cannot be independently disabled or enabled. For example, if Junos OS is restarted, the audit log contains the following information:

```

Dec 20 23:17:35 bilbo syslogd: exiting on signal 14
Dec 20 23:17:35 bilbo syslogd: restart
Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128)
exited with status=1
Dec 20 23:17:42 bilbo /kernel:
Dec 20 23:17:53 init: syslogd (PID 19200) started

```

RELATED DOCUMENTATION

[Login and Logout Events Using SSH](#) | 85

8

CHAPTER

Configuring a Secure Logging Channel

Creating a Secure Logging Channel | **88**

Creating a Secure Logging Channel

This section describes how to place the device in an evaluated configuration to provide an encrypted communication channel over an IPsec VPN tunnel, between a device running Junos OS and a remote external storage server (syslog server).

NOTE: The ssh-rsa authentication method is one of the allowed algorithms in FIPS mode.

[Table 8 on page 89](#) lists all the supported algorithms for the IPsec VPN tunnel.

Table 8: IPsec VPN Tunnel Supported Algorithms

IKE Phase1 Proposal			
Authentication Method	Authentication Algorithm	DH Group	Encryption Algorithm
pre-shared-keys	sha-256	group14	aes-128-cbc
rsa-signatures-2048	sha-384	group19	aes-128-gcm
ecdsa-signatures-256		group20	aes-192-cbc
ecdsa-signatures-384		group24	aes-256-cbc
			aes-256-gcm
			3des-cbc

IPSec Phase2 Proposal			
Authentication Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
hmac-sha1-96	group14	ESP	aes-128-cbc
hmac-sha-256-128	group19		aes-128-gcm
	group20		aes-192-cbc
	group24		aes-192-gcm
			aes-256-cbc
			aes-256-gcm
		3des-cbc	

Configuring a Trusted Path or Channel Between a Device Running Junos OS and a Remote External Storage Server

This section describes the configuration details required to provide an encrypted communication channel between a device running Junos OS and the remote external storage server through an IPsec VPN tunnel.

NOTE: The remote external storage server is a Linux-based syslog server on which the IPsec VPN Tunnel is terminated at the outbound interface Eth1. The log data transferred from the device is sent to the syslog termination interface Eth2 and the StrongSwan application to provide the IPsec VPN capability.

Table 9 on page 90 lists the IPsec VPN tunnel details used in this example.

Table 9: IPsec VPN Tunnel Information

Phase 1 Proposal (P1, IKE)				Phase 2 Proposal (P2, IPSec)			
Authenticat ion Method	Authenticat ion Algorithm	DH Group	Encryption Algorithm	Authenticat ion Algorithm	DH Group (PFS)	Encryption Method	Encryption Algorithm
pre- shared-keys	sha-256	group14	aes-128-cbc	hmac-sha1 -96	group14	ESP	aes-128-cbc

Figure 1 on page 90 illustrates the encrypted communication channel between a device running Junos OS and a remote external storage server. An IPsec tunnel is established between a devices egress interface (Intf-1) and a remote syslog server outbound interface (Eth1). Data is then forwarded internally on the remote external storage server from its outbound interface Eth1; that is, the VPN endpoint to Eth2.

Figure 1: IPsec VPN Tunnel

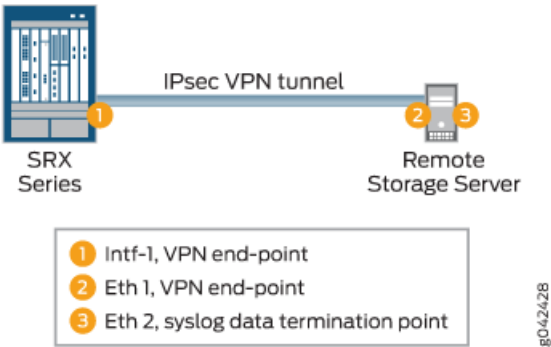


Table 10 on page 91 provides the interface and IP configuration details used in this example.

Table 10: Interface and IP Configuration Details for the Trusted Path

Device Running Junos OS	Remote Storage Server
IP Address:	IP Address:
"Intf-2" interface: GE-0/0/1 – IP Address: 198.51.100.2	Eth1: 198.51.100.3
"Intf-1" interface: GE-0/0/2 - IP Address: 198.51.100.1	Eth2: 203.0.113.1
Enable: Syslog logging to remote syslog server	Gateway Eth1: 198.51.100.1
	Tools: SSH and Strongswan (for IPsec VPN)

To configure the trusted path or channel between a device running Junos OS and a remote external storage server:

1. Enable stream logging for traffic logs.

```
[edit security]
user@host#set log cache
user@host#set log mode event
user@host#set log source-address 198.51.100.2
user@host#set log stream STREAM category all
user@host#set log stream STREAM host 203.0.113.1
```

NOTE: 192.168.2.1 is the IP address of the syslog server outbound interface at which the IPsec VPN tunnel is terminated, and 20.20.20.2 is the IP address of the syslog server interface for which log data is destined.

2. Enable syslog on the device.

```
[edit system]
user@host# set syslog user * any emergency
user@host# set syslog host 203.0.113.1 any any
user@host# set syslog file SYSLOG any any
user@host# set syslog file SYSLOG_COMMANDS interactive-commands error
user@host# set syslog file traffic-log any any
user@host# set syslog file traffic-log match RT_FLOW_SESSION
user@host# set syslog source-address 198.51.100.2
```

3. Enable VPN on the device.

IKE setup:

```
[edit security]
user@host# set ike proposal IKE_Proposal authentication-method pre-shared-keys
user@host# set ike proposal IKE_Proposal dh-group group14
user@host# set ike proposal IKE_Proposal authentication-algorithm sha-256
user@host# set ike proposal IKE_Proposal encryption-algorithm aes-128-cbc
user@host# set ike policy IKE_Policy mode main
user@host# set ike policy IKE_Policy proposals IKE_Proposal
user@host# prompt ike policy IKE_Policy pre-shared-key ascii-text 12345
user@host# set ike gateway GW ike-policy IKE_Policy
user@host# set ike gateway GW address 198.51.100.3
user@host# set ike gateway GW local-identity inet 198.51.100.1
user@host# set ike gateway GW external-interface ge-0/0/2
user@host# set ike gateway GW version v2-only
```

IPsec setup:

```
[edit security ipsec]
user@host# set proposal IPsec_Proposal protocol esp
root@host# set proposal IPsec_Proposal authentication-algorithm hmac-sha1-96
root@host# set proposal IPsec_Proposal encryption-algorithm aes-128-cbc
root@host# set policy IPsec_Policy perfect-forward-secrecy keys group14
root@host# set policy IPsec_Policy proposals IPsec_Proposal
root@host# set vpn VPN bind-interface st0.0
root@host# set vpn VPN ike gateway GW
root@host# set vpn VPN ike ipsec-policy IPsec_Policy
root@host# set vpn VPN establish-tunnels immediately
```

4. Perform the following additional configurations on the device.

IKE trace log:

```
[edit security ike]
root@host# set traceoptions file IKE_Trace
root@host# set traceoptions file size 10000000
root@host# set ike traceoptions flag all
```

Flow trace:

```
[edit security flow ]
root@host# set traceoptions file DEBUG
```

```
root@host# set traceoptions file size 1000000
root@host# set traceoptions flag all
```

Route options:

```
[edit ]
root@host# set routing-options static route 203.0.113.2/24 qualified-next-hop st0.0 preference 1
```

Address book configuration:

```
[edit security address-book]
root@host# set global address trustLAN 198.51.100.0/24
root@host# set global address unTrustLAN 198.51.100.3/24
```

Zone configuration:

```
[edit security zones]
root@host# set security-zone trustZone host-inbound-traffic system-services all
root@host# set security-zone trustZone host-inbound-traffic protocols all
root@host# set security-zone trustZone interfaces ge-0/0/1.0
root@host# set security-zone unTrustZone host-inbound-traffic system-services all
root@host# set security-zone unTrustZone host-inbound-traffic protocols all
root@host# set security-zone unTrustZone interfaces st0.0
root@host# set security-zone unTrustZone interfaces ge-0/0/2.0
```

Policy configuration:

```
[edit security policies]
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 match source-address trustLAN
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 match destination-address
  unTrustLAN
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 match application any
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 then permit
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 then log session-init
root@host# set from-zone trustZone to-zone unTrustZone policy Policy1 then log session-close
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 match source-address unTrustLAN
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 match destination-address trustLAN
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 match application any
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 then permit
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 then log session-init
root@host# set from-zone unTrustZone to-zone trustZone policy Policy1 then log session-close
```

RELATED DOCUMENTATION

[Configuring SSH on the Evaluated Configuration | 47](#)

[Sample Syslog Server Configuration on a Linux System | 50](#)

9

CHAPTER

Configuring VPNs

Configuring VPN on a Device Running Junos OS | 96

Configuring VPN on a Device Running Junos OS

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 98](#)
- [Configuring an IPsec VPN with an RSA Signature for IKE Authentication on page 104](#)
- [Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication on page 108](#)

Figure 2 on page 96 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 2: VPN Topology

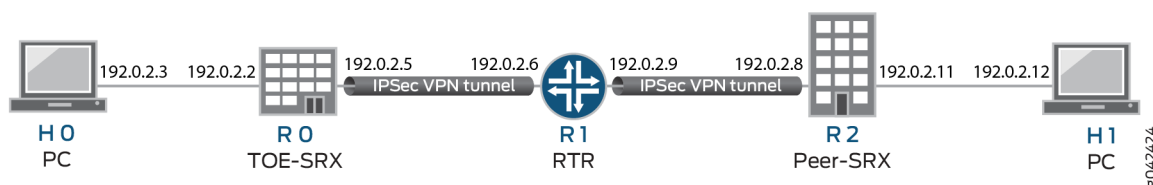


Table 11 on page 97 provides a complete list of the supported IKE protocols, tunnel modes, Phase 1 negotiation mode, authentication method or algorithm, encryption algorithm, DH groups supported for the IKE authentication and encryption (Phase1, IKE Proposal), and for IPsec authentication and encryption (Phase2, IPsec Proposal). The listed protocols, modes, and algorithms are supported and required for 20.4R1 Common Criteria.

Table 11: 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
						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-sha1-96	group14	ESP	3des-cbc
IKEv2			hmac-sha-256-128	group19		aes-128-cbc
				group20		aes-128-gcm
				group24		aes-192-cbc
						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 12 on page 98](#)

Table 12: 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 13 on page 105](#).

Table 13: 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 14 on page 108](#).

Table 14: 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
```

RELATED DOCUMENTATION

[Sample Syslog Server Configuration on a Linux System | 50](#)

[Understanding a Security Flow Policy on a Device Running Junos OS | 116](#)

[IPsec VPN Feature Guide for Security Devices](#)

10

CHAPTER

Configuring Security Flow Policies

Understanding a Security Flow Policy on a Device Running Junos OS | **116**

Understanding a Security Flow Policy on a Device Running Junos OS

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 116](#)
- [Configuring a Security Policy in Firewall Discard Mode on page 117](#)
- [Configuring a Security Flow Policy in IPsec Protect Mode on page 117](#)

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](#)

11

CHAPTER

Configuring Traffic Filtering Rules

Overview | **120**

Understanding Protocol Support | **120**

Configuring Traffic Filter Rules | **122**

Configuring Default Deny-All and Reject Rules | **123**

Logging the Dropped Packets Using Default Deny-all Option | **124**

Configuring Mandatory Reject Rules for Invalid Fragments and Fragmented IP Packets | **125**

Configuring Default Reject Rules for Source Address Spoofing | **126**

Configuring Default Reject Rules with IP Options | **126**

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 8 on page 89](#).

Table 15: Network Traffic Protocols and Fields

Protocol or RFC	Fields
ICMPv4 - RFC 792, Internet Control Message Protocol version 4	<ul style="list-style-type: none"> • Type • Code

Table 15: Network Traffic Protocols and Fields (*continued*)

Protocol or RFC	Fields
ICMPv6 - RFC 4443, Internet Control Message Protocol version 6	<ul style="list-style-type: none"> • Type • Code
IPv4 - RFC 791, Internet Protocol	<ul style="list-style-type: none"> • Source address • Destination address • Transport Layer Protocol
IPv6 - RFC 2460, Internet Protocol	<ul style="list-style-type: none"> • Source address • Destination address • Transport Layer Protocol
TCP - RFC 793, Transmission Control Protocol	<ul style="list-style-type: none"> • Source port • Destination port
UDP - RFC 768, User Datagram Protocol	<ul style="list-style-type: none"> • 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](#) | 122

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](#) | 120

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.

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.

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.

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 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.

Before you begin, log in with your root account to an SRX Series device running Junos OS Release 20.4R1.

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
```

12

CHAPTER

Configuring Network Attacks

Configuring IP Teardrop Attack Screen | **130**

Configuring TCP Land Attack Screen | **131**

Configuring ICMP Fragment Screen | **133**

Configuring Ping-Of-Death Attack Screen | **134**

Configuring tcp-no-flag Attack Screen | **136**

Configuring TCP SYN-FIN Attack Screen | **138**

Configuring TCP fin-no-ack Attack Screen | **139**

Configuring UDP Bomb Attack Screen | **141**

Configuring UDP CHARGEN DoS Attack Screen | **141**

Configuring TCP SYN and RST Attack Screen | **143**

Configuring ICMP Flood Attack Screen | **145**

Configuring TCP SYN Flood Attack Screen | **147**

Configuring TCP Port Scan Attack Screen | **148**

Configuring UDP Port Scan Attack Screen | **150**

Configuring IP Sweep Attack Screen | **152**

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
```

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](#) | 155

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
```

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
```

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
```

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

```

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](#) | 155

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](#) | 155

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
```


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](#) | 155

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](#) | 155

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](#) | 155

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](#) | 155

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](#) | 155

13

CHAPTER

Configuring the IDP Extended Package

[IDP Extended Package Configuration Overview](#) | **155**

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](#)

14

CHAPTER

Configuring Clustering Mode

Understanding Cluster Mode | **157**

Configuring L2 HA Link Encryption tunnel | **157**

Configuring PKI based L2 HA Link Encryption tunnel | **163**

Understanding Cluster Mode

The Administrator of the TOE might set up the cluster mode for High Availability (HA) by connecting ge-0/0/1 on node 0 to ge-0/0/1 on node 1. The factory-default configuration does not include HA configuration. To enable HA, if the physical interfaces used by HA have some configurations, these configurations need to be removed. The two hosts constituting a chassis cluster must have identical configuration except for one being configured to node 0 and the other to node 1.

The TOE has a dedicated physical interface which acts as the fxp0 interface for the HA management of the TOE. The fxp1 interface for HA control link is ge-0/0/1. The fabric interface may be defined by the Administrator. After the cluster has been defined and set up by the Administrator, the two devices constituting a chassis cluster have identical cluster-id but different node ID as one host must be node 0 and the other one node 1. For SRX345 and SRX380 devices, the ge-0/0/1 interface on node 1 changes to ge-5/0/1.

The node 1 rennumbers its interfaces by adding the total number of system FPCs to the original FPC number of the interface. The renumbering constant for SRX345 and SRX380 is 5 which results in the node 0 interface name remaining ge-0/0/0 and the node 1 interface name being renamed to ge-5/0/0. The fabric interface remains Administrator-defined.

With L2 HA link encryption tunnel, any Security Sensitive Parameters (Critical Security Parameters) exchanged over the control link between the two chassis in cluster mode is protected using IPsec. Using IPsec for internal communication between nodes, the configuration information and IKE HA messages that passes through the chassis cluster link from the primary node to the secondary node is protected from active and passive eavesdropping. Without the internal IPsec key, an attacker cannot gain privilege access or observe traffic.

RELATED DOCUMENTATION

Configuring L2 HA Link Encryption tunnel

- Physically connect the two devices and ensure that they are the same models.
- Connect the dedicated control ports on node 0 and node 1.
- Connect the user defined fabricated ports on node 0 and node 1.

To configure two chassis in cluster mode, follow the below steps.

1. Zeroize both the SRX devices before you use for cluster. If the devices are already in cluster mode please make sure you disable them before zeroize.

For information on how to disable chassis cluster, see [Disabling a Chassis Cluster](#)

2. Delete the web management services.

```
user@host# delete system services web-management https
```

3. Configure FIPS mode and bring up the devices in FIPS mode.

```
[edit]
```

```
user@host# set groups global system fips level 2
```

```
[edit]
```

```
user@host# set groups global system root-authentication plain-textpassword
```

```
New password: type password here
```

```
Retype new password: retype password here
```

```
[edit]
```

```
user@host# commit
```

```
user@host> request system reboot
```

4. Configure device 1 with standard cluster commands for operating in cluster mode as node0.

```
[edit]
```

```
user@host# set groups node0 system host-name node0-host-name
```

```
user@host# set groups node0 system backup-router gateway-address
```

```
user@host# set groups node0 system backup-router destination value
```

```
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
```

```
user@host# set groups node1 system host-name node1-host-name
```

```
user@host# set groups node1 system backup-router gateway-address
```

```
user@host# set groups node1 system backup-router destination value
```

```
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
```

```
user@host# set apply-groups global
```

```
user@host# set apply-groups "$(node)
```

```
user@host# delete apply-groups re0
```

```
user@host# set system ports console log-out-on-disconnect
```

```
user@host# set chassis cluster reth-count 5
```

```
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
```

```
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

```
user@host# commit
```

```
user@host> set chassis cluster cluster-id 1 node 0 reboot
```

See

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

5. After the device 1 is up, configure HA link encryption as shown in sample configuration below, commit and reboot. device 1 needs to be configured with both node0 and node1 HA link encryption configuration before commit and reboot.

[edit]

```
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-method
pre-shared-keys
user@host# set groups node0 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-cbc
user@host# set groups node0 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node0 security ike policy IKE_POL_PSK pre-shared-key ascii-text
```

New ascii-text (secret): juniper

Retype new ascii-text (secret): juniper

```
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-method
pre-shared-keys
user@host# set groups node1 security ike proposal IKE_PROP_PSK dh-group group20
```

```

user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node1 security ike policy IKE_POL_PSK pre-shared-key ascii-text

```

New ascii-text (secret): juniper

Retype new ascii-text (secret): juniper

```

user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-5/0/3
user@host# commit
user@host>request system reboot

```

6. To proceed further with device 2 configuration and commit, you need to ensure device1 and device 2 are not reachable to each other. One way to achieve this is to power off device 1 at this point.
7. Configure device 2 with standard cluster command for operating in cluster mode as node1

[edit]

```

user@host# set groups node0 system host-name node0-host-name
user@host# set groups node0 system backup-router gateway-address
user@host# set groups node0 system backup-router destination value
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
user@host# set groups node1 system host-name node1-host-name
user@host# set groups node1 system backup-router gateway-address
user@host# set groups node1 system backup-router destination value
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
user@host# set apply-groups global
user@host# set apply-groups "$(node)"
user@host# delete apply-groups re0

```



```

user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit
user@host> set chassis cluster cluster-id 1 node 1 reboot

```

See

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

8. After the device 2 is up, configure HA link encryption as shown in sample configuration below on device 2. Device 2 needs to be configured with both node0 and node1 HA link encryption configuration. Commit on node1 (device 2), and finally reboot node1 (device 2).

[edit]

```

user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-method
    pre-shared-keys
user@host# set groups node0 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PSK authentication-algorithm
    sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-cbc
user@host# set groups node0 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node0 security ike policy IKE_POL_PSK pre-shared-key ascii-text

```

New ascii-text (secret): juniper

Retype new ascii-text (secret): juniper

```

user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
    hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
    aes-256-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
    group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups node1 security ike traceoptions file ikelog

```

```

user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-method
pre-shared-keys
user@host# set groups node1 security ike proposal IKE_PROP_PSK dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PSK authentication-algorithm
sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PSK encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy IKE_POL_PSK proposals IKE_PROP_PSK
user@host# prompt groups node1 security ike policy IKE_POL_PSK pre-shared-key ascii-text
New ascii-text (secret): juniper
Retype new ascii-text (secret): juniper

user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PSK
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK authentication-algorithm
hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK encryption-algorithm
aes-256-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PSK lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK perfect-forward-secrecy keys
group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PSK proposals IPSEC_PROP_PSK
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PSK
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-5/0/3
user@host# commit
user@host> request system reboot

```

9. Power ON node0 (device 1).

10. Both the nodes will be in cluster mode with HA link encryption enabled.

NOTE: To enable HA link encryption on node1 in step 6, the other node needs to be in lost state for the commit to go through. So this timing needs to be taken care by you, else step 6 needs to be redone until enabling HA link encryption on node1 commit goes through.

Configuring PKI based L2 HA Link Encryption tunnel

- Physically connect the two devices and ensure that they are the same models.
- Connect the dedicated control ports on node 0 and node 1.
- Connect the user defined fabricated ports on node 0 and node 1.

To configure two chassis in cluster mode, follow the below steps.

1. Zeroize both the SRX devices before you use for cluster. If the devices are already in cluster mode please make sure you disable them before zeroize.

For information on how to disable chassis cluster, see [Disabling a Chassis Cluster](#)

2. Delete the web management services.

```
user@host# delete system services web-management https
```

3. Configure FIPS mode and bring up the devices in FIPS mode.

```
[edit]
```

```
user@host# set groups global system fips level 2
```

```
[edit]
```

```
user@host# set groups global system root-authentication plain-textpassword
```

```
New password: type password here
```

```
Retype new password: retype password here
```

```
[edit]
```

```
user@host# commit
```

```
user@host> request system reboot
```

4. Configure device 1 with standard cluster commands for operating in cluster mode as node0. This requires a reboot.

```
[edit]
```

```
user@host# set groups node0 system host-name node0-host-name
```

```
user@host# set groups node0 system backup-router gateway-address
```

```
user@host# set groups node0 system backup-router destination value
```

```
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
```

```
user@host# set groups node1 system host-name node1-host-name
```

```
user@host# set groups node1 system backup-router gateway-address
```

```
user@host# set groups node1 system backup-router destination value
```

```
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
```

```
user@host# set apply-groups global
```

```

user@host# set apply-groups "$(node)
user@host# delete apply-groups re0
user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit
user@host> set chassis cluster cluster-id 1 node 0 reboot

```

See

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

5. After the device 1 is up, configure HA link encryption as shown in sample configuration below, commit and reboot. device 1 needs to be configured with both node0 and node1 HA link encryption configuration before commit and reboot.

```

[edit]
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security pki traceoptions file pkilog
user@host# set groups node0 security pki traceoptions file size 100m
user@host# set groups node0 security pki traceoptions flag all
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-method
    rsa-signatures
user@host# set groups node0 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc
user@host# set groups node0 security ike policy IKE_POL_PKI mode main
user@host# set groups node0 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node0 security ike policy IKE_POL_PKI certificate local-certificate pkicert
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI authentication-algorithm
    hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
    aes-128-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI perfect-forwardsecrecy keys
    group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption

```

```

user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
user@host# set groups node0 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node0 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of
    certificate authority>
user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check crl url <CRL
    distribution point for certificate authority>
user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node0 interfaces st0 unit 0 family inet
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security pki traceoptions file pkilog
user@host# set groups node1 security pki traceoptions file size 100m
user@host# set groups node1 security pki traceoptions flag all
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-method
    rsa-signatures
user@host# set groups node1 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy IKE_POL_PKI mode main
user@host# set groups node1 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node1 security ike policy IKE_POL_PKI certificate local-certificate pkicert
user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm
    hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
    aes-128-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI perfect-forward-secrecy keys
    group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
user@host# set groups node1 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node1 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of
    certificate authority>
user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check crl url <CRL
    distribution point for certificate authority>

```

```

user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node1 interfaces st0 unit 0 family inet
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-5/0/3
user@host# commit
user@host> clear security pki node-local local-certificate all
user@host> clear security pki node-local certificate-request all
user@host> clear security pki node-local key-pair all
user@host> clear security pki crl all
user@host> clear security pki ca-certificate all
user@host> request security pki node-local generate-key-pair certificate-id pkicert type rsa size
2048

```

```

root@vm# curl "http://<PKI-Server-IP>/certsrv/certnew.cer?
ReqID=CACert=0=bin" -o /tmp/dut_ca.cer
root@vm# scp /tmp/dut_ca.cer root@node0-host-name:/var/tmp

```

```

user@host> request security pki ca-certificate load ca-profile S2S_PKI filename/var/tmp/ dut_ca.cer
user@host> show security pki ca-certificate

```

```

root@vm# curl "http://PKI-Server-IP/certsrv/certcrl.crl?Renewal=0=bin"
-o /tmp/dut.crl
root@vm# scp /tmp/dut.crl root@node0-host-name:/var/tmp

```

```

user@host> request security pki crl load ca-profile S2S_PKI filename /var/tmp/dut.crl
user@host> show security pki crl
user@host> request security pki node-local generate-certificate-request certificate-id pkicert subject
CN=testdut,OU=QA,O=JuniperNetworks,L=CNRD,ST=Beijing,C=CN domainname dut.juniper.net
ip-address 129.16.0.1 email dut@juniper.net

```

```

root@vm# rm -rf /cert
root@vm# mkdir /cert
root@vm# chmod 777 /cert
root@vm# echo -----BEGIN CERTIFICATE REQUEST-----copy-generatedkey-----
END CERTIFICATE REQUEST----- > /cert/dsakey
root@vm# cat /cert/dsakey
root@vm# chmod 777 /cert/dsakey
root@vm# chmod o+w /tftpboot

```

```

root@vm# rm -f /etc/xinetd.d/tftp.org
root@vm# cp /etc/xinetd.d/tftp /etc/xinetd.d/tftp.org
root@vm# sed -e 's/server_args.*/server_args = -s \tftpboot -c/g' /etc/
xinetd.d/tftp > /etc/xinetd.d/tftp.mdf
root@vm# mv -f /etc/xinetd.d/tftp.mdf /etc/xinetd.d/tftp
root@vm# systemctl enable tftp.service
root@vm# /bin/systemctl restart xinetd.service
root@vm# mv -f /etc/xinetd.d/tftp.org /etc/xinetd.d/tftp
root@vm# dir /tftpboot/pki.tcl
root@vm# /bin/cp /tftpboot/pki.tcl /cert/
root@vm# chmod 775 /cert/pki.tcl
root@vm# /cert/pki.tcl PKI-Server-IP /cert/dsakey /cert/dut.cer
root@vm# scp /cert/dut.cer root@node0-host-name:/var/tmp

```

```

user@host> clear security pki node-local local-certificate all
user@host> request security pki node-local local-certificate load filename /var/tmp/dut.cer
certificate-id pkicert
user@host> request system reboot

```

6. To proceed further with device 2 configuration and commit, you need to ensure device1 and device 2 are not reachable to each other. One way to achieve this is to power off device 1 at this point.
7. Configure device 2 with standard cluster command for operating in cluster mode as node1. This requires a reboot.

```

[edit]
user@host# set groups node0 system host-name node0-host-name
user@host# set groups node0 system backup-router gateway-address
user@host# set groups node0 system backup-router destination value
user@host# set groups node0 interfaces fxp0 unit 0 family inet address node0-ip-address
user@host# set groups node1 system host-name node1-host-name
user@host# set groups node1 system backup-router gateway-address
user@host# set groups node1 system backup-router destination value
user@host# set groups node1 interfaces fxp0 unit 0 family inet address node1-ip-address
user@host# set apply-groups global
user@host# set apply-groups "$(node)"
user@host# delete apply-groups re0
user@host# set system ports console log-out-on-disconnect
user@host# set chassis cluster reth-count 5
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# commit

```

```
user@host> set chassis cluster cluster-id 1 node 1 reboot
```

See

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-verification.html

8. After the device 2 is up, configure HA link encryption as shown in sample configuration below on device 2. Device 2 needs to be configured with both node0 and node1 HA link encryption configuration before commit and reboot.

[edit]

```
user@host# set groups node0 security ike traceoptions file ikelog
user@host# set groups node0 security ike traceoptions file size 100m
user@host# set groups node0 security ike traceoptions flag all
user@host# set groups node0 security ike traceoptions level 15
user@host# set groups node0 security pki traceoptions file pkilog
user@host# set groups node0 security pki traceoptions file size 100m
user@host# set groups node0 security pki traceoptions flag all
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-method
    rsa-signatures
user@host# set groups node0 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node0 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256
user@host# set groups node0 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc
user@host# set groups node0 security ike policy IKE_POL_PKI mode main
user@host# set groups node0 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node0 security ike policy IKE_POL_PKI certificate local-certificate pkicert
user@host# set groups node0 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node0 security ike gateway S2S_GW version v2-only
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm
    hmac-sha1-96
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
    aes-128-cbc
user@host# set groups node0 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI perfect-forwardsecrecy keys
    group20
user@host# set groups node0 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node0 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node0 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node0 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
user@host# set groups node0 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node0 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of
    certificate authority>
user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check crl url <CRL
    distribution point for certificate authority>
```



```

user@host# set groups node0 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node0 interfaces st0 unit 0 family inet
user@host# set groups node1 security ike traceoptions file ikelog
user@host# set groups node1 security ike traceoptions file size 100m
user@host# set groups node1 security ike traceoptions flag all
user@host# set groups node1 security ike traceoptions level 15
user@host# set groups node1 security pki traceoptions file pkilog
user@host# set groups node1 security pki traceoptions file size 100m
user@host# set groups node1 security pki traceoptions flag all
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-method
    rsa-signatures
user@host# set groups node1 security ike proposal IKE_PROP_PKI dh-group group20
user@host# set groups node1 security ike proposal IKE_PROP_PKI authentication-algorithm sha-256
user@host# set groups node1 security ike proposal IKE_PROP_PKI encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy IKE_POL_PKI mode main
user@host# set groups node1 security ike policy IKE_POL_PKI proposals IKE_PROP_PKI
user@host# set groups node1 security ike policy IKE_POL_PKI certificate local-certificate pkicert
user@host# set groups node1 security ike gateway S2S_GW ike-policy IKE_POL_PKI
user@host# set groups node1 security ike gateway S2S_GW version v2-only
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI protocol esp
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI authenticationalgorithm
    hmac-sha1-96
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI encryptionalgorithm
    aes-128-cbc
user@host# set groups node1 security ipsec proposal IPSEC_PROP_PKI lifetime-seconds 200
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI perfect-forward-secrecy keys
    group20
user@host# set groups node1 security ipsec policy IPSEC_POL_PKI proposals IPSEC_PROP_PKI
user@host# set groups node1 security ipsec vpn S2S_VPN ha-link-encryption
user@host# set groups node1 security ipsec vpn S2S_VPN ike gateway S2S_GW
user@host# set groups node1 security ipsec vpn S2S_VPN ike ipsec-policy IPSEC_POL_PKI
user@host# set groups node1 security pki ca-profile S2S_PKI ca-identity S2S_PKI_CA1
user@host# set groups node1 security pki ca-profile S2S_PKI enrollment url <Enrollment URL of
    certificate authority>
user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check url <CRL
    distribution point for certificate authority>
user@host# set groups node1 security pki ca-profile S2S_PKI revocation-check disable
user@host# set groups node1 interfaces st0 unit 0 family inet
user@host# set groups global interfaces fab0 fabric-options member-interfaces ge-0/0/3
user@host# set groups global interfaces fab1 fabric-options member-interfaces ge-5/0/3
user@host# commit
user@host> clear security pki node-local local-certificate all
user@host> clear security pki node-local certificate-request all

```

```

user@host> clear security pki node-local key-pair all
user@host> clear security pki crl all
user@host> clear security pki ca-certificate all
user@host> request security pki node-local generate-key-pair certificate-id pkicert type rsa size
2048

```

```

root@vm# curl "http://PKI-Server-IP/certsrv/certnew.cer?
ReqID=CACert=0=bin" -o /tmp/aux_ca.cer
root@vm# scp /tmp/aux_ca.cer root@node1-host-name:/var/tmp

```

```

user@host> request security pki ca-certificate load ca-profile S2S_PKI filename /var/tmp/aux_ca.cer
user@host> show security pki ca-certificate

```

```

root@vm# curl "http://PKI-Server-IP/certsrv/certcrl.crl?Renewal=0=bin"
-o /tmp/aux.crl
root@vm# scp /tmp/aux.crl root@node1-host-name:/var/tmp

```

```

user@host> request security pki crl load ca-profile S2S_PKI filename /var/tmp/aux.crl
user@host> show security pki crl
user@host> request security pki node-local generate-certificate-request certificate-id pkicert subject
CN=testaux,OU=QA,O=JuniperNetworks,L=CNRD,ST=Beijing,C=CN domainname aux.juniper.net
ip-address 130.16.0.1 email aux@juniper.net

```

```

root@vm# rm -rf /cert
root@vm# mkdir /cert
root@vm# chmod 777 /cert
root@vm# echo -----BEGIN CERTIFICATE REQUEST-----copy-generatedkey-----
END CERTIFICATE REQUEST----- > /cert/dsakey
root@vm# cat /cert/dsakey
root@vm# chmod 777 /cert/dsakey
root@vm# chmod o+w /tftpboot
root@vm# rm -f /etc/xinetd.d/tftp.org
root@vm# cp /etc/xinetd.d/tftp /etc/xinetd.d/tftp.org
root@vm# sed -e 's/server_args.*/server_args = -s \/tftpboot -c/g' /etc/
xinetd.d/tftp > /etc/xinetd.d/tftp.mdf
root@vm# mv -f /etc/xinetd.d/tftp.mdf /etc/xinetd.d/tftp
root@vm# systemctl enable tftp.service
root@vm# /bin/systemctl restart xinetd.service
root@vm# mv -f /etc/xinetd.d/tftp.org /etc/xinetd.d/tftp

```

```

root@vm# dir /tftpboot/pki.tcl
root@vm# /bin/cp /tftpboot/pki.tcl /cert/
root@vm# chmod 775 /cert/pki.tcl
root@vm# /cert/pki.tcl PKI-Server-IP /cert/dsakey /cert/aux.cer
root@vm# scp /cert/aux.cer root@node1-host-name:/var/tmp

```

```

user@host> clear security pki node-local local-certificate all
user@host> request security pki node-local local-certificate load filename /var/tmp/aux.cer
certificate-id pkicert
user@host> request system reboot

```

9. Power ON node0 (device 1).

10. Both the nodes will be in cluster mode with PKI HA link encryption enabled.

NOTE: To enable HA link encryption on node1 in step 6, the other node needs to be in lost state for the commit to go through. So this timing needs to be taken care by you, else step 6 needs to be redone until enabling HA link encryption on node1 commit goes through. Also above example shows, configuring PKI based L2 HA link encryption tunnel with RSA. However, we can also use ECDSA with key size 256 and 384.

15

CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 173

Understanding FIPS Self-Tests

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 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
verifix: cannot update verifix for /usr/lib/libext_db.so.3: Too many links
verifix: cannot update verifix for /usr/lib/libpsu.so.3: Too many links
verifix: cannot update verifix for /usr/lib/libxml2.so.3: Too many links
verifix: cannot update verifix for /usr/lib/libyaml.so.3: Too many links
verifix: cannot update verifix for /var/jailetc/mime.types: No such file or
directory
verifix: cannot update verifix 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 cp1d0
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 Oocteon 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 Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: no fingerprint for
file='/sbin/kats/cannot-exec' fsid=83 fileid=5048524 gen=1 uid=0 pid=1073
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: 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 Junos OS in FIPS Mode of Operation*

16

CHAPTER

Configuration Statements

`checksum-validate` | **180**

Sample Code Audits of Configuration Changes | **181**

`data-length` | **184**

`destination-option` | **185**

`extension-header` | **186**

`header-type` | **187**

`home-address` | **188**

`identification` | **189**

`icmpv6` (Security IDP Custom Attack) | **190**

`ihl` (Security IDP Custom Attack) | **191**

`option-type` | **192**

`reserved` (Security IDP Custom Attack) | **193**

`routing-header` | **194**

`sequence-number` (Security IDP ICMPv6 Headers) | **195**

`type` (Security IDP ICMPv6 Headers) | **196**

checksum-validate

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| [IDP Extended Package Configuration Overview](#)

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*

data-length

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]
```

Release Information

Statement introduced in Junos OS Release 9.3.

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.

RELATED DOCUMENTATION

| [IDP Extended Package Configuration Overview](#)

destination-option

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

extension-header

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

header-type

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]

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| [IDP Extended Package Configuration Overview](#)

home-address

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

identification

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

icmpv6 (Security IDP Custom Attack)

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

ihl (Security IDP Custom Attack)

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

option-type

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]

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

reserved (Security IDP Custom Attack)

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

routing-header

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| [IDP Extended Package Configuration Overview](#)

sequence-number (Security IDP ICMPv6 Headers)

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*

type (Security IDP ICMPv6 Headers)

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]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D30.

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.

RELATED DOCUMENTATION

| *IDP Extended Package Configuration Overview*