

Junos[®] OS

Common Criteria Evaluated Guide for MX240, MX480, MX960, MX2010, and MX2020 Devices

Published
2020-04-13

Release
19.1R2

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 Evaluated Guide for MX240, MX480, MX960, MX2010, and MX2020 Devices

19.1R2

Copyright © 2020 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 | vii

Documentation and Release Notes | vii

Documentation Conventions | vii

Documentation Feedback | x

Requesting Technical Support | x

Self-Help Online Tools and Resources | xi

Creating a Service Request with JTAC | xi

1

Overview

Understanding the Common Criteria Evaluated Configuration | 13

Understanding Common Criteria | 13

Supported Platforms | 14

Understanding Junos OS in FIPS Mode | 14

About the Cryptographic Boundary on Your Device | 15

How FIPS Mode Differs from Non-FIPS Mode | 15

Validated Version of Junos OS in FIPS Mode | 15

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms | 16

Terminology | 16

Supported Cryptographic Algorithms | 17

Identifying Secure Product Delivery | 19

Understanding Management Interfaces | 20

2

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in Common Criteria and FIPS | 22

Security Administrator Role and Responsibilities | 23

FIPS User Role and Responsibilities | 23

What Is Expected of All FIPS Users | 24

Understanding the Operational Environment for Junos OS in FIPS Mode | 24

Hardware Environment for Junos OS in FIPS Mode | 25

Software Environment for Junos OS in FIPS Mode | 25

Critical Security Parameters | 26

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 29

Downloading Software Packages from Juniper Networks | 30

Installing Software on a MX Series Routers with a Single Routing Engine | 31

Understanding Zeroization to Clear System Data for FIPS Mode | 34

Why Zeroize? | 35

When to Zeroize? | 35

Zeroizing the System | 36

Enabling FIPS Mode | 37

Configuring Security Administrator and FIPS User Identification and Access | 39

Configuring Security Administrator Access | 39

Configuring FIPS User Login Access | 41

3

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Authorized Administrator | 45

Configuring a Network Device Collaborative Protection Profile Authorized Administrator | 47

Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle Session | 49

Configuring Session Termination | 49

Sample Output for Local Administrative Session Termination | 50

Sample Output for Remote Administrative Session Termination | 51

Sample Output for User Initiated Termination | 51

4

Configuring SSH and Console Connection

Configuring a System Login Message and Announcement | 53

Configuring SSH on the Evaluated Configuration for NDcPP | 54

Limiting the Number of User Login Attempts for SSH Sessions | 56

5

Configuring the Remote Syslog Server

Syslog Server Configuration on a Linux System | 59

Configuring Event Logging to a Local File | 59

Configuring Event Logging to a Remote Server | 59

Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server | 60

6

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration | 68

Configuring Audit Log Options for MX240, MX480, MX960, MX2010, and MX2020 Devices | 68

Sample Code Audits of Configuration Changes | 69

7

Configuring Event Logging

Event Logging Overview | 85

Configuring Event Logging to a Local File | 86

Interpreting Event Messages | 86

Logging Changes to Secret Data | 88

Login and Logout Events Using SSH | 89

Logging of Audit Startup | 89

8

Configuring VPNs

Overview of VPNEP | 92

Section | ?

Configuring IPsec VPN Extended Package (EP) | 92

IPsec VPN Configuration with Reference Identifier | 98

Sample IPsec VPN Configuration with IPv4 Address as Reference Identifier | 99

Sample IPsec VPN Configuration with FQDN as Reference Identifier | 106

Sample Configuration for Distinguished Name as Reference Identifier | 113

Generating Certificate Signing Request (CSR) | 124

Configuring Firewall Rules | 125

9

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 133

10

Operational Commands

request system zeroize | 141

request vmhost zeroize no-forwarding | 143

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vii
- Documentation Conventions | vii
- Documentation Feedback | x
- Requesting Technical Support | x

Use this guide to configure and evaluate MX240, MX480, MX960, MX2010, and MX2020 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 viii defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 on page viii 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 | **13**

Understanding Junos OS in FIPS Mode | **14**

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms | **16**

Identifying Secure Product Delivery | **19**

Understanding Management Interfaces | **20**

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:

- NDcPPv2—https://www.commoncriteriaportal.org/files/ppfiles/PPP_ND_V2.0.pdf
- VPNEP—<https://www.niap-ccevs.org/Profile/Info.cfm?id=382>

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

NOTE: For regulatory compliance information about Common Criteria, and FIPS for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

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/>.

Target of Evaluation (TOE) is a device or system subjected to evaluation based on Collaborative Protection Profile (cPP).

NOTE: On MX240, MX480, MX960, MX2010, and MX2020 devices, Junos OS Release 19.1R2 is certified for Common Criteria with FIPS mode enabled on the devices.

Supported Platforms

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

- Routing Engine (RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G, or RE-S-X6-64G and REMX2K-X8-64G) and service PIC (MSMPC for VPNEP) have to be installed on MX240, MX480, MX960, MX2010, and MX2020 to qualify NDcPPv2 and VPNEP.

RELATED DOCUMENTATION

[Identifying Secure Product Delivery | 19](#)

Understanding Junos OS in FIPS Mode

IN THIS SECTION

- [About the Cryptographic Boundary on Your Device | 15](#)
- [How FIPS Mode Differs from Non-FIPS Mode | 15](#)
- [Validated Version of Junos OS in FIPS Mode | 15](#)

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, the Juniper Networks RE-S-1800X4, RE-MX2000-1800X4, REMX2K-1800-32G, RE-S-X6-64G, and REMX2K-X8-64G Routing Engines on Juniper Networks MX Series 3D Universal Edge Routers running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

Operating MX Series routers in a FIPS 140-2 Level 1 environment requires enabling and configuring FIPS mode on the routers from the Junos OS command-line interface (CLI).

The *Security-Administrator* enables FIPS mode in Junos OS Release 19.1R2 and sets up keys and passwords for the system and other *FIPS users*.

About the Cryptographic Boundary on Your Device

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a router. Junos OS in FIPS mode prevents the cryptographic module from executing 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. Do not configure a Virtual Chassis in FIPS mode.

How FIPS Mode Differs from Non-FIPS Mode

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

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and MD5 are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters long.

Validated Version of Junos OS in FIPS Mode

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

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- Terminology | 16
- Supported Cryptographic Algorithms | 17

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

Terminology

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.

Security Administrator—For Common Criteria, user accounts in the TOE have the following attributes: user identity (user name), authentication data (password), and role (privilege). The Security Administrator is associated with the defined login class “security-admin”, which has the necessary permission set to permit the administrator to perform all tasks necessary to manage the Junos OS.

NDcPP—Collaborative Protection Profile for Network Devices, version 2.1.

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. For details, see [“Understanding the Operational Environment for Junos OS in FIPS Mode” on page 24](#).

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. MX devices are certified at FIPS 140-2 Level 1.

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos OS in FIPS mode complies with FIPS 140-2 Level 1.

FIPS maintenance role—The role the security administrator assumes to perform physical maintenance or logical maintenance services such as hardware or software diagnostics. For FIPS 140-2 compliance, the security administrator zeroizes the Routing Engine on entry to and exit from the FIPS maintenance role to erase all plain-text secret and private keys and unprotected CSPs.

NOTE: The FIPS maintenance role is not supported on Junos OS in FIPS mode.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of Junos OS modules. For details, see [“Understanding FIPS Self-Tests” on page 133](#).

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 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.

Supported Cryptographic Algorithms

[Table 3 on page 17](#) summarizes the high level protocol algorithm support.

Table 3: Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	<ul style="list-style-type: none"> ECDH-sha2-nistp256 ECDH-sha2-nistp384 ECDH-sha2-nistp521 	Host (module): <ul style="list-style-type: none"> ECDSA P-256 Client (user): <ul style="list-style-type: none"> ECDSA P-256 ECDSA P-384 ECDSA P-521 	<ul style="list-style-type: none"> AES CTR 128 AES CTR 256 AES CBC 128 AES CBC 256 	<ul style="list-style-type: none"> HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

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

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods 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 or 256 bits to encrypt and decrypt data in blocks of 128 bits.

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, and P-521 curves 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, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.

SHA-256 and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, and SHA-512 produces a 512-bit hash digest.

RELATED DOCUMENTATION

[Understanding FIPS Self-Tests | 133](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 34](#)

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](#) | 13

Understanding Management Interfaces

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

- Local Management Interfaces—The RJ-45 console port on the 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.

RELATED DOCUMENTATION

| [Understanding the Common Criteria Evaluated Configuration](#) | 13

2

CHAPTER

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in Common Criteria and FIPS | 22

Understanding the Operational Environment for Junos OS in FIPS Mode | 24

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 29

Downloading Software Packages from Juniper Networks | 30

Installing Software on a MX Series Routers with a Single Routing Engine | 31

Understanding Zeroization to Clear System Data for FIPS Mode | 34

Zeroizing the System | 36

Enabling FIPS Mode | 37

Configuring Security Administrator and FIPS User Identification and Access | 39

Understanding Roles and Services for Junos OS in Common Criteria and FIPS

IN THIS SECTION

- [Security Administrator Role and Responsibilities | 23](#)
- [FIPS User Role and Responsibilities | 23](#)
- [What Is Expected of All FIPS Users | 24](#)

For Common Criteria, user accounts in the TOE have the following attributes: user identity (user name), authentication data (password) and role (privilege). The Security Administrator is associated with the defined login class “security-admin”, which has the necessary permission set to permit the administrator to perform all tasks necessary to manage Junos OS. Administrative users (Security Administrator) must provide unique identification and authentication data before any administrative access to the system is granted.

Security Administrator roles and responsibilities are as follows:

1. Security Administrator can administer the TOE locally and remotely.
2. Create, modify, delete administrator accounts, including configuration of authentication failure parameters.
3. Re-enable an Administrator account.
4. Responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product.

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode 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 (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 is role-based rather than identity-based.

Security administrator performs all FIPS-mode-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode. Security administrator and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode.

Security Administrator Role and Responsibilities

The security administrator is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a router. The security administrator securely installs Junos OS on the router enables FIPS mode, establishes keys and passwords for other users and software modules, and initializes the router before network 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 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, the security administrator is expected to:

- Set the initial root password. The length of the password should be atleast 10 characters.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Examine log and audit files for events of interest.
- Erase user-generated files, keys, and data by zeroizing the router.

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.

FIPS user can view status output but cannot reboot or zeroize the device.

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 routers and documentation in a secure area.
- Deploy routers 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

[Zeroizing the System](#) | 36

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

- [Hardware Environment for Junos OS in FIPS Mode](#) | 25
- [Software Environment for Junos OS in FIPS Mode](#) | 25
- [Critical Security Parameters](#) | 26

A Juniper Networks router running the Juniper Networks Junos operating system (Junos OS) in FIPS mode forms a special type of hardware and software operational environment that is different from the environment of a router in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the router that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the router that requires a cryptographic boundary for FIPS 140-2 compliance is a separate cryptographic module

Cryptographic methods are not a substitute for physical security. The hardware must be located in a secure physical environment. Users of all types must not reveal keys or passwords, or allow written records or notes to be seen by unauthorized personnel.

Software Environment for Junos OS in FIPS Mode

A Juniper Networks router running Junos OS in FIPS mode forms a special type of nonmodifiable operational environment. To achieve this environment on the router, the system prevents the execution of any binary file that was not part of the certified Junos OS in FIPS mode distribution. When a router is in FIPS mode, it can run only Junos OS.

FIPS mode on MX Series routers is available in Junos OS. The Junos OS in FIPS mode software environment is established after the security administrator successfully enables FIPS mode on a router. The Junos OS Release 19.1R2 image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning router.

For FIPS 140-2 compliance, we recommend that you delete all user-created files and data by *zeroizing* the device before enabling FIPS mode.

Enabling FIPS mode disables many of the usual Junos OS protocols and services. In particular, you cannot configure the following services in Junos OS in FIPS mode:

- finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error.

You can use only SSH as a remote access service.

All passwords established for users after upgrading to Junos OS in FIPS mode must conform to Junos OS in FIPS mode specifications. Passwords must be between 10 and 20 characters in length and require the use of at least three of the five defined character sets (uppercase and lowercase letters, digits, punctuation marks, and keyboard characters, such as % and &, not included in the other four categories). Attempts to configure passwords that do not conform to these rules result in an error. All passwords and keys used to authenticate peers must be at least 10 characters in length, and in some cases the length must match the digest size.

NOTE: Do not attach the router to a network until the security administrator completes configuration from the local console connection.

For strict compliance, do not examine core and crash dump information on the local console in Junos OS in FIPS mode because some CSPs might be shown in plain text.

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 router or Routing Engine as a cryptographic module.

Table 4 on page 26 lists CSPs on routers running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroization Method	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.

Table 4: Critical Security Parameters (continued)

CSP	Description	Zeroization Method	Use
SSH-2 session key	<p>Session key used with SSH-2. and as a Diffie-Hellman private key.</p> <p>Encryption: AES-128, AES-256.</p> <p>MACs: HMAC-SHA-1, HMAC SHA-2-256, HMAC SHA2-512.</p> <p>Key exchange: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.</p>	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA256, SHA512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Security administrator authentication key	Hash of the security administrator's password: SHA256, SHA512.	Zeroize command.	Used to authenticate the security administrator to the cryptographic module.
HMAC DRBG seed	Seed for deterministic random bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

In Junos OS in FIPS mode, all CSPs must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the security administrator, you can enter user authentication data in plain text.

BEST PRACTICE: For FIPS compliance, configure the router over SSH connections because they are encrypted connections.

Local passwords are hashed with the SHA256 or SHA512 algorithm. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

RELATED DOCUMENTATION

[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 29](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 34](#)

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

All passwords established for users by the security administrator must conform to the following Junos OS in FIPS mode requirements. Attempts to configure passwords that do not conform to the following specifications result in an error.

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
 - Uppercase letters
 - Lowercase letters
 - Digits
 - Punctuation marks
 - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size.
- **Password encryption.** To change the default encryption method (SHA512) include the **format** statement at the **[edit system login password]** hierarchy level.

Guidelines for strong passwords. Strong, reusable passwords can be based on letters from a favorite phrase or word and then concatenated with other unrelated words, along with added digits and punctuation. In general, a strong password is:

- Easy to remember so that users are not tempted to write it down.
- Made up of mixed alphanumeric characters and punctuation. For FIPS compliance include at least one change of case, one or more digits, and one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Characteristics of weak passwords. Do not use the following weak passwords:

- Words that might be found in or exist as a permuted form in a system files such as **/etc/passwd**.
- The hostname of the system (always a first guess).

- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.
- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**r00t**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

RELATED DOCUMENTATION

Understanding the Operational Environment for Junos OS in FIPS Mode | 24

Downloading Software Packages from Juniper Networks

You can download the following Junos OS software packages from the Juniper Networks website:

- Junos OS for MX devices, Release 19.1R2

NOTE: For MX RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G download **junos-install-mx-x86-64-19.1R2.tgz** and for MX RE-S-X6-64G and REMX2K-X8-64G download **junos-vmhost-install-mx-x86-64-19.1R2.tgz**.

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 Software on a MX Series Routers with a Single Routing Engine

You can use this procedure to upgrade Junos OS on router with a single Routing Engine.

To install software upgrades on a router with a single Routing Engine:

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks” on page 30](#).
2. If you have not already done so, connect to the console port on the router from your management device, and log in to the Junos OS CLI.
3. (Optional) Back up the current software configuration to a second storage option. See the [Junos OS Installation and Upgrade Guide](#) for instructions on performing this task.
4. (Optional) Copy the software package to the router. We recommend that you use FTP to copy the file to the `/var/tmp/` directory.

This step is optional because Junos OS can also be upgraded when the software image is stored at a remote location. These instructions describe the software upgrade process for both scenarios.

5. Install the new package on the device:

For RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G,

```
user@router> request system software add <package>
```

For RE-S-X6-64G and REMX2K-X8-64G,

```
user@router> request vmhost software add <package>
```

Replace *package* with one of the following paths:

NOTE: Trusted update with delayed activation is not supported by TOE.

- For a software package in a local directory on the router, use `/var/tmp/package.tgz`.
- For a software package on a remote server, use one of the following paths, replacing *package* with the software package name.—for example, `junos-vmhost-install-mx-x86-64-19.1R2.tgz`.
 - `ftp://hostname/pathname/package.tgz`
 - `http://hostname/pathname/package.tgz`

6. Reboot the device to load the installation:

For RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G

```
user@router> request system reboot
```

For RE-S-X6-64G and REMX2K-X8-64G

```
user@router> request vmhost reboot
```

7. After the reboot has completed, log in and use the **show version** command to verify that the new version of the software is successfully installed. If you installed the Junos FIPS mode package, verify that the FIPS mode utilities are present—as shown in the following example:

```
user@host> show version
Hostname: host
Model: mx240
Junos: 19.1R2.6
JUNOS OS Kernel 64-bit [20190305.df99236_builder_stable_11]
JUNOS OS libs [20190305.df99236_builder_stable_11]
JUNOS OS runtime [20190305.df99236_builder_stable_11]
JUNOS OS time zone information [20190305.df99236_builder_stable_11]
JUNOS network stack and utilities [20190321.051058_builder_junos_191_r1]
JUNOS libs [20190321.051058_builder_junos_191_r1]
JUNOS OS libs compat32 [20190305.df99236_builder_stable_11]
JUNOS OS 32-bit compatibility [20190305.df99236_builder_stable_11]
JUNOS libs compat32 [20190321.051058_builder_junos_191_r1]
JUNOS runtime [20190321.051058_builder_junos_191_r1]
JUNOS sflow mx [20190321.051058_builder_junos_191_r1]
JUNOS py extensions [20190321.051058_builder_junos_191_r1]
```



```

JUNOS py base [20190321.051058_builder_junos_191_r1]
JUNOS OS crypto [20190305.df99236_builder_stable_11]
JUNOS na telemetry [19.1R2.6]
JUNOS Security Intelligence [20190321.051058_builder_junos_191_r1]
JUNOS mx libs compat32 [20190321.051058_builder_junos_191_r1]
JUNOS mx runtime [20190321.051058_builder_junos_191_r1]
JUNOS common platform support [20190321.051058_builder_junos_191_r1]
JUNOS Openconfig [19.1R2.6]
JUNOS mtx network modules [20190321.051058_builder_junos_191_r1]
JUNOS modules [20190321.051058_builder_junos_191_r1]
JUNOS mx modules [20190321.051058_builder_junos_191_r1]
JUNOS mx libs [20190321.051058_builder_junos_191_r1]
JUNOS SQL Sync Daemon [20190321.051058_builder_junos_191_r1]
JUNOS mtx Data Plane Crypto Support [20190321.051058_builder_junos_191_r1]
JUNOS daemons [20190321.051058_builder_junos_191_r1]
JUNOS mx daemons [20190321.051058_builder_junos_191_r1]
JUNOS Services URL Filter package [20190321.051058_builder_junos_191_r1]
JUNOS Services TLB Service PIC package [20190321.051058_builder_junos_191_r1]
JUNOS Services Telemetry [20190321.051058_builder_junos_191_r1]
JUNOS Services TCP-LOG [20190321.051058_builder_junos_191_r1]
JUNOS Services SSL [20190321.051058_builder_junos_191_r1]
JUNOS Services SOFTWIRE [20190321.051058_builder_junos_191_r1]
JUNOS Services Stateful Firewall [20190321.051058_builder_junos_191_r1]
JUNOS Services RTCOM [20190321.051058_builder_junos_191_r1]
JUNOS Services RPM [20190321.051058_builder_junos_191_r1]
JUNOS Services PCEF package [20190321.051058_builder_junos_191_r1]
JUNOS Services NAT [20190321.051058_builder_junos_191_r1]
JUNOS Services Mobile Subscriber Service Container package
[20190321.051058_builder_junos_191_r1]
JUNOS Services MobileNext Software package [20190321.051058_builder_junos_191_r1]
JUNOS Services Logging Report Framework package
[20190321.051058_builder_junos_191_r1]
JUNOS Services LL-PDF Container package [20190321.051058_builder_junos_191_r1]
JUNOS Services Jflow Container package [20190321.051058_builder_junos_191_r1]
JUNOS Services Deep Packet Inspection package
[20190321.051058_builder_junos_191_r1]
JUNOS Services IPSec [20190321.051058_builder_junos_191_r1]
JUNOS Services IDS [20190321.051058_builder_junos_191_r1]
JUNOS IDP Services [20190321.051058_builder_junos_191_r1]
JUNOS Services HTTP Content Management package
[20190321.051058_builder_junos_191_r1]
JUNOS Services Flowd MS-MPC Software package [20190321.051058_builder_junos_191_r1]
JUNOS Services Crypto [20190321.051058_builder_junos_191_r1]
JUNOS Services Captive Portal and Content Delivery Container package

```

```
[20190321.051058_builder_junos_191_r1]
JUNOS Services COS [20190321.051058_builder_junos_191_r1]
JUNOS AppId Services [20190321.051058_builder_junos_191_r1]
JUNOS Services Application Level Gateways [20190321.051058_builder_junos_191_r1]
JUNOS Services AACL Container package [20190321.051058_builder_junos_191_r1]
JUNOS SDN Software Suite [20190321.051058_builder_junos_191_r1]
JUNOS Extension Toolkit [20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (wrlinux9)
[20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (MXSPC3)
[20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
[20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (MX Common)
[20190321.051058_builder_junos_191_r1]
JUNOS J-Insight [20190321.051058_builder_junos_191_r1]
JUNOS jfirmware [20190321.051058_builder_junos_191_r1]
JUNOS Online Documentation [20190321.051058_builder_junos_191_r1]
JUNOS jail runtime [20190305.df99236_builder_stable_11]
```

RELATED DOCUMENTATION

[Troubleshooting Software Installation](#)

Understanding Zeroization to Clear System Data for FIPS Mode

IN THIS SECTION

- [Why Zeroize? | 35](#)
- [When to Zeroize? | 35](#)

Zeroization completely erases all configuration information on the Routing Engines, including all plain-text passwords, secrets, and private keys for SSH, local encryption, and local authentication.

For RE-S-1800X4, RE-X2000-1800X4, and REMX2K-1800-32G, security administrator initiates the zeroization process by entering the **request system zeroize** operational command.

For RE-S-X6-64G and REMX2K-X8-64G, security administrator initiates the zeroization process by entering the **request vmhost zeroize no-forwarding** operational command.

NOTE: In reference to cryptographic key destruction, TOE does not support delayed key destruction.



CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The router is returned to the factory default state, without any configured users or configuration files.

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 router is not considered a valid FIPS cryptographic module until all critical security parameters (CSPs) have been entered—or reentered—while the router is in FIPS mode.

For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the router.

When to Zeroize?

As security administrator, perform zeroization in the following situations:

- **Before enabling FIPS mode of operation:** To prepare your router for operation as a FIPS cryptographic module, perform zeroization before enabling FIPS mode and before FIPS operation.
- **Before disabling FIPS mode of operation:** To begin repurposing your router for non-FIPS operation, perform zeroization before disabling FIPS mode on the router .

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

RELATED DOCUMENTATION

[Zeroizing the System](#) | 36

Zeroizing the System

To zeroize your device, follow the below procedure:

1. For RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G, from the CLI, enter

```
root@router> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes
re0:
```

For RE-S-X6-64G and REMX2K-X8-64G, from the CLI, enter

```
root@router> request vmhost zeroize no-forwarding
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes

re0:
```

2. To initiate the zeroization process, type **yes** at the prompt:

```
Erase all data, including configuration and log files?   [yes, no] (no)
yes
re0:
-----
warning: zeroizing re0
...
```

...

The entire operation can take considerable time depending on the size of the media, but all critical security parameters (CSPs) are removed within a few seconds. The physical environment must remain secure until the zeroization process is complete.

RELATED DOCUMENTATION

[Enabling FIPS Mode | 37](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 34](#)

Enabling FIPS Mode

When Junos OS is installed on a router and the router is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. When you log in as **root**, your SSH connection is enabled by default.

As security administrator, you must establish a root password conforming to the FIPS password requirements in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 29](#). When you enable FIPS mode in Junos OS on the router, you cannot configure passwords unless they meet this standard.

Local passwords are encrypted with the secure hash algorithm SHA256 or SHA512. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

To enable FIPS mode in Junos OS on the device:

1. Zeroize the device to delete all CSPs before entering FIPS mode. Refer to [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 34](#) section for details.
2. After the device comes up in 'Amnesiac mode', login using username **root** and password "" (blank).

```
FreeBSD/amd64 (Amnesiac) (ttyu0)
login: root
--- JUNOS 19.1-20180131.0 Kernel 64-bit  JNPR-11.0-20180123.155949_fbsd-
root@:~ # cli
root>
```

3. Configure root authentication.

```

root> edit
  Entering configuration mode
[edit]
root# set system root-authentication plain-text-password
New password:
Retype new password:
[edit]
root# commit
commit complete

```

4. Load configuration onto device and commit new configuration.

5. Install **fips-mode** package needed for Routing Engine KATS.

```

root@hostname> request system software add optional://fips-mode.tgz
Verified fips-mode signed by PackageDevelopmentEc_2017 method ECDSA256+SHA256

```

6. Install **jpfe-fips** package needed for MS-MPC line card KATS. (This is only for MX router having MS-MPC line card).

```

root@hostname> request system software add optional://jpfe-fips.tgz
Verified jpfe-fips signed by PackageDevelopmentEc_2017 method ECDSA256+SHA256

```

7. For MX Series devices,

- Configure chassis boundary fips by setting **set system fips chassis level 1** and **commit**.

Device might display the **Encrypted-password must be re-configured to use FIPS compliant hash** warning to delete older CSP in loaded configuration.

8. After deleting and reconfiguring CSPs, commit will go through and device needs reboot to enter FIPS mode.

```

[edit]
root@hostname# commit
Generating RSA key /etc/ssh/fips_ssh_host_key
Generating RSA2 key /etc/ssh/fips_ssh_host_rsa_key
Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
[edit]
system

```

```
reboot is required to transition to FIPS level 1
commit complete
root@hostname# run request system reboot
```

9. After rebooting the device, FIPS self-tests will run and device enters FIPS mode.

```
root@hostname:fips>
```

RELATED DOCUMENTATION

[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 29](#)

Configuring Security Administrator and FIPS User Identification and Access

IN THIS SECTION

- [Configuring Security Administrator Access | 39](#)
- [Configuring FIPS User Login Access | 41](#)

Security administrator and FIPS users perform all configuration tasks for Junos OS in FIPS mode and issue all Junos OS in FIPS mode statements and commands. Security administrator and FIPS user configurations must follow Junos OS in FIPS mode guidelines.

Configuring Security Administrator Access

Junos OS in FIPS mode offers a finer granularity of user permissions than those mandated by FIPS 140-2.

For FIPS 140-2 compliance, any FIPS user with the **secret**, **security**, **maintenance**, and **control** permission bits set is a security administrator. In most cases the **super-user** class suffices for the security administrator.

To configure login access for a security administrator:

1. Log in to the router with the root password if you have not already done so, and enter configuration mode:

```
root@host:fips> configure
  Entering configuration mode
[edit]
root@host:fips#
```

2. Name the user **security-admin** and assign the security administrator a user ID (for example, **6400**, which must be a unique number associated with the login account in the range of 100 through 64000) and a class (for example, **super-user**). When you assign the class, you assign the permissions—for example, **secret**, **security**, **maintenance**, and **control**.

For a list of permissions, see [Understanding Junos OS Access Privilege Levels](#).

```
[edit]
root@host:fips# set system login user username uid value class class-name
```

For example:

```
[edit]
root@host:fips# set system login user security-admin uid 6400 class super-user
```

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on page 29, assign the security administrator a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
root@host:fips# set system login user username uid value class class-name authentication (plain-test-password | encrypted-password)
```

For example:

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

4. Optionally, display the configuration:

```
[edit]
```



```

root@host:fips# edit system
[edit system]
root@host:fips# show
login {
  user security-admin {
    uid 6400;
    authentication {
      encrypted-password "<cipher-text>"; ## SECRET-DATA
    }
    class super-user;
  }
}

```

5. If you are finished configuring the router, commit the configuration and exit:

```

[edit]
root@host:fips# commit
commit complete
root@host:fips# exit
root@host:fips> exit

```

Otherwise, go on to [“Configuring FIPS User Login Access” on page 41](#).

Configuring FIPS User Login Access

A **fips-user** is defined as any FIPS user that does not have the **secret**, **security**, **maintenance**, and **control** permission bits set.

As the security administrator you set up FIPS users. FIPS users cannot be granted permissions normally reserved for the security administrator—for example, permission to zeroize the system.

To configure login access for a FIPS user:

1. Log in to the router with your security administrator password if you have not already done so, and enter configuration mode:

```

security-admin@host:fips> configure
  Entering configuration mode
[edit]
security-admin@host:fips#

```

2. Give the user, a username, and assign the user a user ID (for example, **6401**, which must be a unique number in the range of 1 through 64000) and a class. When you assign the class, you assign the permissions—for example, **clear**, **configure**, **network**, **resetview**, and **view-configuration**.

For a list of permissions, see [Understanding Junos OS Access Privilege Levels](#).

```
[edit]
root@host:fips# set system login user username uid value class read-only
```

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on page 29, assign the FIPS user a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
root@host:fips# set system login user username uid value class read-only authentication (plain-text-password
| encrypted-password)
```

4. Optionally, display the configuration:

```
[edit]
security-admin@host:fips# edit system
[edit system]
security-admin@host:fips# show
login {
  user fips-user1 {
    uid 6401;
    authentication {
      encrypted-password "<cipher-text>"; ## SECRET-DATA
    }
    class read-only;
  }
}
```

5. If you are finished configuring the router, commit the configuration and exit:

```
[edit]
security-admin@host:fips# commit
security-admin@host:fips> exit
```

RELATED DOCUMENTATION

| [Understanding Roles and Services for Junos OS in Common Criteria and FIPS](#) | 22

3

CHAPTER

Configuring Administrative Credentials and Privileges

Understanding the Associated Password Rules for an Authorized Administrator | 45

Configuring a Network Device Collaborative Protection Profile Authorized
Administrator | 47

Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle
Session | 49

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 hashing algorithm for user passwords can be either SHA256 or SHA512 (SHA512 is the default hashing algorithm).

[edit]

```
administrator@host# set system login password format sha256
```

NOTE: The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048, 3072, and 4092 modulus bit length) key-types.

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

Configuring a Network Device Collaborative 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 NDcPPv2 authorized administrator must have all permissions, including the ability to change the router configuration.

To configure an authorized administrator:

NOTE: When the **log-key-changes** configuration statement is enabled and committed (with the commit command in configuration mode), Junos OS logs the changes to the set of authorized SSH keys for each user (including the keys that were added or removed). Junos OS logs the differences since the last time the **log-key-changes** configuration statement was enabled. If the **log-key-changes** configuration statement was never enabled, then Junos OS logs all the authorized SSH keys.

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

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

2. Configure the hashed algorithm for plain-text passwords as sha512.

```
[edit]
root@host# set system login password format sha512
```

3. Commit the changes.

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

4. Define your NDcPPv2 user authorized administrator.

```
[edit]
```

```
root@host# set system login user NDcPPv2-user full-name
Common-Criteria-NDcPPv2-Authorized-Administrator class security-admin authentication
encrypted-password <password>
```

5. Load an SSH key file that was previously generated using ssh-keygen. This command loads RSA (SSH version 2), or ECDSA (SSH version 2).

```
[edit]
root@host#set system root-authentication load-key-file url:filename
```

6. Set the log-key-changes configuration statement to log when SSH authentication keys are added or removed.

```
[edit]
root@host#set system services ssh log-key-changes
```

7. Commit the changes.

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

NOTE: The root password should be reset following the change to sha256 / sha512 for the password storage format. This ensures the new password is protected using a sha256 / sha512 hash. To reset the root password, use **set system root-authentication plain-text-password password** command, and confirm the new password when prompted.

RELATED DOCUMENTATION

Understanding the Associated Password Rules for an Authorized Administrator | 45

Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle Session

IN THIS SECTION

- [Configuring Session Termination | 49](#)
- [Sample Output for Local Administrative Session Termination | 50](#)
- [Sample Output for Remote Administrative Session Termination | 51](#)
- [Sample Output for User Initiated Termination | 51](#)

Configuring Session Termination

Terminate the session after the security administrator specifies inactive timeout period.

1. Set the idle timeout.

```
[edit]  
administrator@host# set system login class security-admin idle-timeout 2
```

2. Configure the login access privileges.

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

3. Commit the configuration.

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

```
commit complete
```

4. Set the password.

```
[edit]
administrator@host# set system login user NDcPPv2-user authentication plain-text-password
New password:
Retype new password:
```

5. Define login class.

```
[edit]
administrator@host# set system login user NDcPPv2-user class security-admin
```

6. Commit the configuration.

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

```
commit complete
```

Sample Output for Local Administrative Session Termination

```
con host
Trying a.b.c.d...
'autologin': unknown argument ('set ?' for help).
Connected to device.example.com
Escape character is '^]'.

Type the hot key to suspend the connection: <CTRL>Z
FreeBSD/amd64 (host) (ttyu0)
login: NDcPPv2-user
Password:
Last login: Sun Jun 23 22:42:27 from 10.224.33.70

--- JUNOS 19.1R2.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@host> Warning: session will be closed in 1 minute if there is no
activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

```
FreeBSD/amd64 (host) (ttyu0)
```

Sample Output for Remote Administrative Session Termination

```
ssh NDcPPv2-user@host
Password:
Last login: Sun Jun 23 22:48:05 2019
--- JUNOS 19.1R2.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@host> exit

Connection to host closed.
ssh NDcPPv2-user@host
Password:
Last login: Sun Jun 23 22:50:50 2019 from 10.224.33.70
--- JUNOS 19.1R2.6 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@host> Warning: session will be closed in 1 minute if there is no
activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

Connection to host closed.
```

Sample Output for User Initiated Termination

```
ssh NDcPPv2-user@host
Password:
Last login: Sun Jun 23 22:48:05 2019
--- JUNOS 19.1R2.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@host> exit

Connection to host closed.
```

4

CHAPTER

Configuring SSH and Console Connection

Configuring a System Login Message and Announcement | 53

Configuring SSH on the Evaluated Configuration for NDcPP | 54

Limiting the Number of User Login Attempts for SSH Sessions | 56

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 through console or management interface, 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

Configuring SSH on the Evaluated Configuration for NDcPP

SSH through remote management interface allowed in the evaluated configuration. If the existing ssh connection is broken unintentionally, for example reboot, re-initiate the connection after the device is up. There is no mechanism to retain an existing or established connection, which is broken.

This topic describes how to configure SSH for remote management of TOE. The following algorithms that needs to be configured to validate SSH for NDcPP.

To configure SSH on the TOE:

1. Specify the permissible SSH host-key algorithms for the system services.

```
[edit]
user@host#set system services ssh hostkey-algorithm ssh-ecdsa
user@host#set system services ssh hostkey-algorithm no-ssh-dss
user@host#set system services ssh hostkey-algorithm ssh-rsa
```

2. Specify the SSH key-exchange for Diffie-Hellman keys for the system services.

```
[edit]
user@host#set system services ssh key-exchange dh-group14-sha1
user@host#set system services ssh key-exchange ecdh-sha2-nistp256
user@host#set system services ssh key-exchange ecdh-sha2-nistp384
user@host#set system services ssh key-exchange ecdh-sha2-nistp521
```

3. Specify all the permissible message authentication code algorithms for SSHv2

```
[edit]
user@host#set system services ssh macs hmac-sha1
user@host#set system services ssh macs hmac-sha2-256
user@host#set system services ssh macs hmac-sha2-512
```

4. Specify the ciphers allowed for protocol version 2.

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

```
user@host#set system services ssh ciphers aes128-ctr
user@host#set system services ssh ciphers aes256-ctr
```

Supported SSH hostkey algorithm:

ssh-ecdsa	Allow generation of ECDSA host-key
ssh-rsa	Allow generation of RSA host-key

Supported SSH key-exchange algorithm:

dh-group14-sha1	The RFC 4253 mandated group14 with SHA1 hash
ecdh-sha2-nistp256	The EC Diffie-Hellman on nistp256 with SHA2-256
ecdh-sha2-nistp384	The EC Diffie-Hellman on nistp384 with SHA2-384
ecdh-sha2-nistp521	The EC Diffie-Hellman on nistp521 with SHA2-512

Supported MACs algorithm:

hmac-sha1	Hash-based MAC using Secure Hash Algorithm (SHA1)
hmac-sha2-256	Hash-based MAC using Secure Hash Algorithm (SHA2)
hmac-sha2-512	Hash-based MAC using Secure Hash Algorithm (SHA2)

Supported SSH ciphers algorithm:

aes128-cbc	128-bit AES with Cipher Block Chaining
aes128-ctr	128-bit AES with Counter Mode
aes256-cbc	256-bit AES with Cipher Block Chaining
aes256-ctr	256-bit AES with Counter Mode

Limiting the Number of User Login Attempts for SSH Sessions

An administrator may login remotely 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 configure the amount of time the device gets locked after failed attempts. The amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again.

The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.

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

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.

```
[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. Use the **backoff-factor** option to specify the length of the delay in seconds. The range is from 1 through 3, and the default value is 2 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.

You can control user access through SSH. By configuring ssh **root-login deny**, you can ensure the root account remains active and continues to have local administrative privileges to the TOE even if other remote users are logged off.

```
[edit system]  
user@host# set services ssh root-login deny
```

The SSH2 protocol provides secure terminal sessions utilizing the secure encryption. The SSH2 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 of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.

5

CHAPTER

Configuring the Remote Syslog Server

Syslog Server Configuration on a Linux System | 59

Syslog Server Configuration on a Linux System

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 router. 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

Configure audit information to be stored in a local file on the device along with the level of detail using the "syslog" statement. The following must be used to ensure all events detailed in the NDcPP are logged and are stored in a local file named Audit_file in the following example:

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

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 "ssh-rsa xxxxx 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/Audit_file`.

```
[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.

```
$ ssh syslog-mon@NDcPP_TOE -s netconf > test.out
```

NOTE: All logging data received by the remote syslog server is placed in the **test.out** file.

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@nms5-vm-linux2 ~]$ 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+kreBUQjrmr6775RJn9H9YwIxK0xGm4SFnX/Vl4
R+lZ9RqmKH2wodIEM34K0wXEHzAzNZ0loLmaAVqT
syslog-monitor key pair
[host@nms5-vm-linux2 ~]$ eval `ssh-agent`
Agent pid 1453
[host@nms5-vm-linux2 ~]$ 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)

```

```

host@nms5-vm-linux2 ~]$ ssh syslog-mon@starfire -s netconf > test.out
host@nms5-vm-linux2 ~]$ 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'

```

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
.....

```



NOTE: When a SSH connection from the syslog server is not established, no audit data is sent. A new SSH session has to be established for the audit records to be sent to the syslog server. Old records are not forwarded to the syslog server.

6

CHAPTER

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration | **68**

Sample Code Audits of Configuration Changes | **69**

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

- [Configuring Audit Log Options for MX240, MX480, MX960, MX2010, and MX2020 Devices | 68](#)

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

Configuring Audit Log Options for MX240, MX480, MX960, MX2010, and MX2020 Devices

To configure audit log options for MX240, MX480, MX960, MX2010, and MX2020 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. Specify the priority and facility in messages for the system logging facility.

```
[edit system syslog]
```

```
root@host#set file syslog explicit-priority
```

5. Log system messages in a structured format.

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

RELATED DOCUMENTATION

| [Sample Code Audits of Configuration Changes](#) | 69

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 **Audit-File**:

```
[edit system]
syslog {
  file Audit-File {
    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 **Audit-File**:

```
[edit system]
syslog {
  file Audit-File {
    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 "$ABC123";
            # SECRET-DATA
        }
    }
}
radius-server 192.0.2.15 {
    secret "$ABC123" # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file messages {
        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

```

Table 5 on page 71 shows sample for syslog auditing for NDcPPv2:

Table 5: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	How event 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	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
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_COP.1(1)/KeyedHashCMAC	None	None	
FCS_RBG_EXT.1	None	None	
FIA_PMG_EXT.1	None	None	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			<p>Successful Local Login</p> <p>Jan 3 09:59:36 login[7637]: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0</p> <p>Jan 3 09:59:36 login[7637]: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0</p> <p>Unsuccessful Local Login</p> <p>Jan 3 09:57:52 login[7637]: LOGIN_PAM_ AUTHENTICATION_ERROR: Failed password for user root</p> <p>Jan 3 09:57:52 login[7637]: LOGIN_FAILED: Login failed for user root from host ttyu0</p> <p>Successful Remote Login</p> <p>Jan 3 09:32:07 mgd[47035]: UI_AUTH_EVENT: Authenticated user 'test1' assigned to class 'j-read-only' Jan 3 09:32:07 mgd[47035]: UI_LOGIN_EVENT: User 'test1' login, class 'j-read-only' [47035], ssh-connection '10.1.5.153 36784 10.1.2.68 22', client-mode 'cli'</p> <p>Unsuccessful Remote Login</p>

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			Jan 3 09:26:56 sshd: SSHD_LOGIN_FAILED: Login failed for user 'test1' from host '10.1.5.153'

Table 5: Auditable Events (*continued*)

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

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			<p>Successful Local Login</p> <p>Jan 3 09:59:36 login[7637]: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0 Jan 3 09:59:36 login[7637]: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0</p> <p>Unsuccessful Local Login</p> <p>Jan 3 09:57:52 login[7637]: LOGIN_PAM_ AUTHENTICATION_ERROR: Failed password for user root</p> <p>Jan 3 09:57:52 login[7637]: LOGIN_FAILED: Login failed for user root from host ttyu0</p> <p>Successful Remote Login</p> <p>Jan 3 09:32:07 mgd[47035]: UI_AUTH_EVENT: Authenticated user 'test1' assigned to class 'j-read-only' Jan 3 09:32:07 mgd[47035]: UI_LOGIN_EVENT: User 'test1' login, class 'j-read-only' [47035], ssh-connection '10.1.5.153 36784 10.1.2.68 22', client-mode 'cli'</p> <p>Unsuccessful Remote Login</p> <p>Jan 3 09:26:56 sshd:</p>

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			SSHD_LOGIN_FAILED: Login failed for user 'test1' from host '10.1.5.153'
FIA_UAU.7	None	None	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	Dec 28 21:51:21 mgd[8007]: UI_CMDLINE_READ_LINE: User 'root', command 'request vmhost software add /var/tmp/junos- vmhost-install- mx-x86-64-19.1- 20181231.0.tgz no-validate'
FMT_MTD.1/CoreData	None	None	
FMT_SMF.1	All management activities of TSF data	None	Refer to the audit events listed in this table.
FMT_SMR.2	None	None	
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	Dec 28 21:51:21 mgd[8007]: UI_CMDLINE_READ_LINE: User 'root', command 'request vmhost software add /var/tmp/junos- vmhost-install-mx- x86-64-19.1- 20181231.0.tgz no-validate'

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	Apr 22 15:31:37 mgd[11121]: UI_CMDLINE_READ_LINE: User 'root', command 'set date 201904221532.00 Apr 22 15:32:05 mgd[11121]: UI_CMDLINE_READ_LINE: User 'root', command 'show system uptime '
FPT_STM_EXT.1 FTA_SSL_EXT.1 (if "terminate the session is selected)	The termination of a local interactive session by the session locking mechanism.	None	Jan 3 11:59:29 cli: UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'root' exceeded and session terminated
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None	Jan 3 11:26:23 cli: UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'root' exceeded and session terminated
FTA_SSL.4	The termination of an interactive session.	None	Local Jan 3 11:47:25 mgd[52521]: UI_LOGOUT_EVENT: User 'root' logout Remote Jan 3 11:43:33 sshd[52425]: Received disconnect from 10.1.5.153 port 36800:11: disconnected by user
FTA_TAB.1	None	None	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
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.	<p>Initiation of the trusted path</p> <p>Jan 3 12:09:00 sshd[53492]: Accepted keyboard-interactive/pam for root from 10.1.5.153 port 36802 ssh2</p> <p>Termination of the trusted path</p> <p>Jan 3 12:09:03 sshd[53492]: Received disconnect from 10.1.5.153 port 36802:11: disconnected by user Jan 3 12:09:36 sshd:</p> <p>Failure of the trusted path</p> <p>SSHD_LOGIN_FAILED: Login failed for user 'root' from host '10.1.5.153'</p>

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None	<p>Initiation of the trusted path</p> <p>Jan 3 12:09:00 sshd[53492]: Accepted keyboard-interactive/pam for root from 10.1.5.153 port 36802 ssh2</p> <p>Termination of the trusted path</p> <p>Jan 3 12:09:03 sshd[53492]: Received disconnect from 10.1.5.153 port 36802:11: disconnected by user Jan 3 12:09:36 sshd:</p> <p>Failure of the trusted path</p> <p>SSHD_LOGIN_FAILED: Login failed for user 'root' from host '10.1.5.153'</p>
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	<p>Dec 17 15:02:12 sshd[9842]: Unable to negotiate with 10.1.5.153 port 43836: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c</p>

Table 5: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Dec 28 22:20:23 verixec[9371]: cannot validate /packages/db/pkginst.9286/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L=Sunnyvale/O=Juniper Networks/ OU=Juniper CA/CN=PackageProductionTest Ec_2017_NO_DEFECTS/ emailAddress=ca@juniper.net
FIA_X509_EXT.2	None	None	
FPT_TUD_EXT.2	Failure of update	Reason for failure (including identifier of invalid certificate)	Dec 28 22:20:23 verixec[9371]: cannot validate /packages/db/pkginst.9286/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L=Sunnyvale/O=Juniper Networks/ OU=Juniper CA/CN=PackageProductionTest Ec_2017_NO_DEFECTS/ emailAddress=ca@juniper.net
FMT_MOF.1/Functions	None	None	
FMT_MOF.1/Services	None	None	
FMT_MTD.1/CryptoKeys	None	None	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_AFL.1	Administrator lockout due to excessive authentication failures	None	Jan 3 08:13:59 sshd: SSHD_LOGIN_ATTEMPTS_THRESHOLD: Threshold for unsuccessful authentication attempts (2) reached by user 'test1'
FPT_RPL.1	Detected replay attempt	None	Apr 15 10:05:16.142910 MKA actor #0 received duplicate or delayed PDU Apr 15 10:05:16.142932 MKA actor #0 received MKPDU, SCI 3C:94:D5:A0:A0:07/1, MI 27:D7:9F:97:53: CF:EF:86:00:52:C1:78, MN 1530

RELATED DOCUMENTATION

Configuring Audit Log Options in the Evaluated Configuration | 68

7

CHAPTER

Configuring Event Logging

Event Logging Overview | **85**

Configuring Event Logging to a Local File | **86**

Interpreting Event Messages | **86**

Logging Changes to Secret Data | **88**

Login and Logout Events Using SSH | **89**

Logging of Audit Startup | **89**

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 following events:

- Changes to secret key data in the configuration.
- Committed changes.
- Login/logout of users.
- System startup.
- Failure to establish an SSH session.
- Establishment/termination of an SSH session.
- Changes to the (system) time.
- Termination of a remote session by the session locking mechanism.
- Termination of an interactive session.

In addition, Juniper Networks recommends that logging also:

- Capture all changes to the configuration.
- Store logging information remotely.

RELATED DOCUMENTATION

| [Interpreting Event Messages](#) | 86

Configuring Event Logging to a Local File

You can configure storing of audit information to a local file with the **syslog** statement. This example stores logs in a file named **Audit-File**:

```
[edit system]
syslog {
  file Audit-File;
}
```

RELATED DOCUMENTATION

| [Event Logging Overview](#) | 85

Interpreting Event Messages

The following output shows a sample event message.

```
Feb 27 02:33:04 bm-a mgd[6520]: UI_LOGIN_EVENT: User 'security-officer' login, class 'j-super-user' [6520],
ssh-connection ", client-mode 'cli'
Feb 27 02:33:49 bm-a mgd[6520]: UI_DBASE_LOGIN_EVENT: User 'security-officer' entering configuration
mode
Feb 27 02:38:29 bm-a mgd[6520]: UI_CMDLINE_READ_LINE: User 'security-officer', command 'run show log
Audit_log | grep LOGIN
```

[Table 6 on page 87](#) 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 6: Fields in Event Messages

Field	Description	Examples
timestamp	<p>Time when the message was generated, in one of two representations:</p> <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. 	<p>Feb 27 02:33:04 is the timestamp expressed as local time in the United States.</p> <p>2012-02-27T09:17:15.719Z is 2:33 AM UTC on 27 Feb 2012.</p>
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

Logging Changes to Secret Data

The following are examples of audit logs of events that change the secret data. Whenever there is a change in the configuration example, the syslog event should capture the below logs:

```
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]
```

Everytime a configuration is updated or changed, the syslog should capture these logs:

```
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]
```

For more information about configuring parameters and managing log files, see the *Junos OS System Log Messages Reference*.

RELATED DOCUMENTATION

| [Interpreting Event Messages](#) | 86

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](#) | 86

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](#) | 89

8

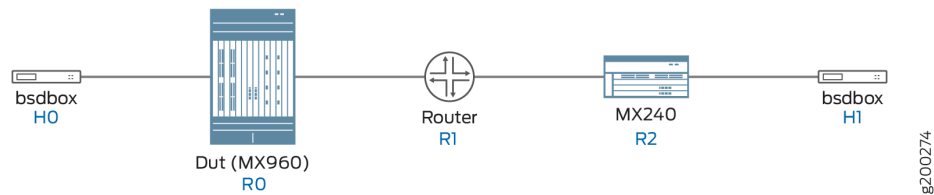
CHAPTER

Configuring VPNs

Overview of VPNEP | 92

Overview of VPNEP

This Extended Package (EP) describes security requirements for a VPN Gateway. This is defined to be a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. The EP is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats to VPN Gateway technology. However, this EP is not complete in itself, but rather extends the collaborative Protection Profile for Network Devices (NDcPPv2) and the collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDcPPv2 and/or FWcPP



Configuring IPsec VPN Extended Package (EP)

In this section, you configure devices running Junos OS for IPsec VPN using a preshared key as the IKE authentication method.

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

1. Configure the IPsec rule on R0.

```
[edit]
security-administrator@host:fips# set services service-set ipsec_ss_ms_4_0_0_1 next-hop-service
inside-service-interface ms-4/0/0.1
security-administrator@host:fips# set services service-set ipsec_ss_ms_4_0_0_1 next-hop-service
outside-service-interface ms-4/0/0.2
security-administrator@host:fips# set services service-set ipsec_ss_ms_4_0_0_1 ipsec-vpn-options
local-gateway 20.1.1.1
security-administrator@host:fips# set services service-set ipsec_ss_ms_4_0_0_1 ipsec-vpn-rules
vpn_rule_ms_4_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 from
source-address 10.1.1.0/24
```

```

security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 from
    destination-address 40.1.1.0/24
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 then
    remote-gateway 30.1.1.2
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 then dynamic
    ike-policy ike_policy_ms_4_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 then dynamic
    ipsec-policy ipsec_policy_ms_4_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 term term1 then
    anti-replay-window-size 4096
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_4_0_0_1 match-direction input
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0_1 protocol
    esp
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0_1
    encryption-algorithm aes-192-cbc
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0_1
    lifetime-seconds 7200
security-administrator@host:fips# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0_1
    perfect-forward-secrecy keys group20
security-administrator@host:fips# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0_1 proposals
    ipsec_proposal_ms_4_0_0_1
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0_1
    authentication-method pre-shared-keys
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0_1
    lifetime-seconds 7200
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0_1 dh-group
    group20
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0_1
    encryption-algorithm aes-192-cbc
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy_ms_4_0_0_1 version 2
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy_ms_4_0_0_1 proposals
    ike_proposal_ms_4_0_0_1
security-administrator@host:fips# prompt services ipsec-vpn ike policy ike_policy_ms_4_0_0_1 pre-shared-key
    ascii-text
New ascii-text (secret):
Retype new ascii-text (secret):

```

NOTE: In FIPS mode, use **prompt** command for setting pre-shared-key. Type-in pre-shared-key in ASCII format when prompted for secret as below:

```
security-administrator@host:fips# prompt services ipsec-vpn ike policy ike_policy_ms_4_0_0_1
pre-shared-key ascii-text
New ascii-text (secret): xxxxxxxx
Retype new ascii-text (secret): xxxxxxxx
```

```
security-administrator@host:fips# set services ipsec-vpn traceoptions file ipsec_log1
security-administrator@host:fips# set services ipsec-vpn traceoptions level all
security-administrator@host:fips# set services ipsec-vpn traceoptions flag all
security-administrator@host:fips# set services ipsec-vpn establish-tunnels immediately
```

2. Configure Routing options on R0.

```
[edit]
security-administrator@host:fips# set routing-options static route 40.1.1.0/24 next-hop ms-4/0/0.
security-administrator@host:fips# set routing-options static route 10.1.1.0/24 next-hop 10.1.1.2
security-administrator@host:fips# set routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
```

3. Configure Interfaces on R0.

```
[edit]
security-administrator@host:fips# set interfaces ms-4/0/0 unit 0 family inet
security-administrator@host:fips# set interfaces ms-4/0/0 unit 1 family inet
security-administrator@host:fips# set interfaces ms-4/0/0 unit 1 family inet6
security-administrator@host:fips# set interfaces ms-4/0/0 unit 1 service-domain inside
security-administrator@host:fips# set interfaces ms-4/0/0 unit 2 family inet
security-administrator@host:fips# set interfaces ms-4/0/0 unit 2 family inet6
security-administrator@host:fips# set interfaces ms-4/0/0 unit 2 service-domain outside
security-administrator@host:fips# set interfaces ge-7/0/1 unit 0 family inet address 10.1.1.2/24
security-administrator@host:fips# set interfaces ge-7/0/3 unit 0 family inet address 20.1.1.1/24
```

4. Configure Interfaces on R1.

```
[edit]
security-administrator@host:fips# set interfaces ge-2/1/2 unit 0 family inet address 20.1.1.2/24
security-administrator@host:fips# set interfaces ge-2/1/3 unit 0 family inet address 30.1.1.1/24
```

5. Configure the IPsec rule on R2.

```
[edit]
security-administrator@host:fips# set services service-set ipsec_ss_ms_3_0_0_1 next-hop-service
    inside-service-interface ms-3/0/0.1
security-administrator@host:fips# set services service-set ipsec_ss_ms_3_0_0_1 next-hop-service
    outside-service-interface m s-3/0/0.2
security-administrator@host:fips# set services service-set ipsec_ss_ms_3_0_0_1 ipsec-vpn-options
    local-gateway 30.1.1.2
security-administrator@host:fips# set services service-set ipsec_ss_ms_3_0_0_1 ipsec-vpn-rules
    vpn_rule_ms_3_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 from
    source-address 40.1.1.0/24
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 from
    destination-address 10.1.1.0/24
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 then
    remote-gateway 20.1.1.1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 then dynamic
    ike-policy ike_policy_ms_3_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 then dynamic
    ipsec-policy ipsec_policy_ms_3_0_0_1
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 term term1 then
    anti-replay-window-size 4096
security-administrator@host:fips# set services ipsec-vpn rule vpn_rule_ms_3_0_0_1 match-direction input
[edit]
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_3_0_0_1 protocol
    esp
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_3_0_0_1
    encryption-algorithm aes-192-cbc
security-administrator@host:fips# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_3_0_0_1
    lifetime-seconds 7200
security-administrator@host:fips# set services ipsec-vpn ipsec policy ipsec_policy_ms_3_0_0_1
    perfect-forward-secrecy keys group20
security-administrator@host:fips# set services ipsec-vpn ipsec policy ipsec_policy_ms_3_0_0_1 proposals
    ipsec_proposal_ms_3_0_0_1
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_3_0_0_1
    authentication-method pre-shared-keys
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_3_0_0_1
    lifetime-seconds 7200
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_3_0_0_1 dh-group
    group20
security-administrator@host:fips# set services ipsec-vpn ike proposal ike_proposal_ms_3_0_0_1
    encryption-algorithm aes-192-cbc
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy_ms_3_0_0_1 version 2
```

```
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy_ms_3_0_0_1 proposals
ike_proposal_ms_3_0_0_1
security-administrator@host:fips# prompt services ipsec-vpn ike policy ike_policy_ms_4_0_0_1 pre-shared-key
ascii-text
New ascii-text (secret):
Retype new ascii-text (secret):
```

NOTE: In FIPS mode, use **prompt** command for setting pre-shared-key. Type-in pre-shared-key in ASCII format when prompted for secret as below:

```
security-administrator@host:fips# prompt services ipsec-vpn ike policy ike_policy_ms_4_0_0_1
pre-shared-key ascii-text
New ascii-text (secret): xxxxxxxx
Retype new ascii-text (secret): xxxxxxxx
```

```
security-administrator@host:fips# set services ipsec-vpn traceoptions file ipsec_log1
security-administrator@host:fips# set services ipsec-vpn traceoptions level all
security-administrator@host:fips# set services ipsec-vpn traceoptions flag all
security-administrator@host:fips# set services ipsec-vpn establish-tunnels immediately
```

6. Configure Routing options on R2.

```
[edit]
security-administrator@host:fips# set routing-options static route 10.1.1.0/24 next-hop ms-3/0/0.1.
security-administrator@host:fips# set routing-options static route 40.1.1.0/24 next-hop 40.1.1.1
security-administrator@host:fips# set routing-options static route 20.1.1.0/24 next-hop 30.1.1.1
```

7. Configure interfaces on R2.

```
[edit]
security-administrator@host:fips# set interfaces ge-0/0/1 unit 0 family inet address 30.1.1.2/24.
security-administrator@host:fips# set interfaces ge-0/0/4 unit 0 family inet address 40.1.1.1/24
security-administrator@host:fips# set interfaces ms-3/0/0 unit 0 family inet
security-administrator@host:fips# set interfaces ms-3/0/0 unit 1 family inet
security-administrator@host:fips# set interfaces ms-3/0/0 unit 1 family inet6
security-administrator@host:fips# set interfaces ms-3/0/0 unit 1 service-domain inside
security-administrator@host:fips# set interfaces ms-3/0/0 unit 2 family inet
security-administrator@host:fips# set interfaces ms-3/0/0 unit 2 family inet6
security-administrator@host:fips# set interfaces ms-3/0/0 unit 2 service-domain outside
```

Sample output for IPsec VPN:


```
security-administrator@host:fips>show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
30.1.1.2	Matured	be51a9075821ab2a	26887fa8c98a9f45	IKEv2

```
security-administrator@host:fips>show services ipsec-vpn ipsec security-associations
```

```
Service set: ipsec_ss_ms_4_0_0_1, IKE Routing-instance: default
Rule: vpn_rule_ms_4_0_0_1, Term: term1, Tunnel index: 1
Local gateway: 20.1.1.1, Remote gateway: 30.1.1.2
IPSec inside interface: ms-4/0/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
NATT Detection: Not Detected, NATT keepalive interval: 0
```

Direction	SPI	AUX-SPI	Mode	Type	Protocol
inbound	3602080831	0	tunnel	dynamic	ESP
outbound	2594649153	0	tunnel	dynamic	ESP

Supported encryption algorithms for IPsec:

aes-128-cbc	AES-CBC 128-bit encryption algorithm
aes-128-gcm	AES-GCM 128-bit encryption algorithm with 16 octet ICV
aes-192-cbc	AES-CBC 192-bit encryption algorithm
aes-192-gcm	AES-GCM 192-bit encryption algorithm with 16 octet ICV
aes-256-cbc	AES-CBC 256-bit encryption algorithm
aes-256-gcm	AES-GCM 256-bit encryption algorithm with 16 octet ICV

Supported encryption algorithms for IKE:

aes-128-cbc	AES-CBC 128-bit encryption algorithm
aes-192-cbc	AES-CBC 192-bit encryption algorithm
aes-256-cbc	AES-CBC 256-bit encryption algorithm

IKE DH groups supported:

group14	Diffie-Hellman Group14
group19	Diffie-Hellman Group19
group20	Diffie-Hellman Group20

IPsec authentication algorithm:

hmac-sha256-128	HMAC-SHA256-128 authentication algorithm
-----------------	--

IKE authentication algorithms:

sha256	SHA 256-bit authentication algorithm
sha-384	SHA 384-bit authentication algorithm
sha1	SHA1 authentication algorithm

Supported authentication methods:

ecdsa-signatures-256	ECDSA signatures (254 bit modulus)
ecdsa-signatures-384	ECDSA signatures (384 bit modulus)
pre-shared-keys	Preshared keys
rsa-signatures	RSA signatures

NOTE: For more information on IKE/IPsec lifetime, see https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/lifetime-seconds-edit-services.html.

IPsec VPN Configuration with Reference Identifier

MX devices support the following reference identifiers for IPsec VPN configuration:

- IP address
- FQDN
- Distinguished Name

Sample IPsec VPN Configuration with IPv4 Address as Reference Identifier

DUT:

```
[edit]
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy1 local-id ipv4_addr 11.0.1.2
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy1 remote-id ipv4_addr 11.0.1.1
```

```
[edit]
security-administrator@host:fips# commit
commit complete
```

```
[edit]
security-administrator@host:fips# show services | display set

set services service-set ssl next-hop-service inside-service-interface
ms-2/0/0.1
set services service-set ssl next-hop-service outside-service-interface
ms-2/0/0.2
set services service-set ssl ipsec-vpn-options local-gateway 11.0.1.2
set services service-set ssl ipsec-vpn-rules rule1
set services ipsec-vpn rule rule1 term term1 from source-address 80.0.0.0/16
set services ipsec-vpn rule rule1 term term1 from destination-address
30.0.0.0/16
set services ipsec-vpn rule rule1 term term1 then remote-gateway 11.0.1.1
set services ipsec-vpn rule rule1 term term1 then dynamic ike-policy
ike_policy1
set services ipsec-vpn rule rule1 term term1 then dynamic ipsec-policy
ipsec_policy1
set services ipsec-vpn rule rule1 term term1 then anti-replay-window-size
4096
set services ipsec-vpn rule rule1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy1 perfect-forward-secrecy
keys group20
set services ipsec-vpn ipsec policy ipsec_policy1 proposals ipsec_proposal1
```

```

set services ipsec-vpn ike proposal ike_proposal1 authentication-method
rsa-signatures
set services ipsec-vpn ike proposal ike_proposal1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal1 authentication-algorithm
sha-256
set services ipsec-vpn ike proposal ike_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ike policy ike_policy1 version 2
set services ipsec-vpn ike policy ike_policy1 proposals ike_proposal1
set services ipsec-vpn ike policy ike_policy1 local-id ipv4_addr 11.0.1.2
set services ipsec-vpn ike policy ike_policy1 local-certificate r1_cert_id
set services ipsec-vpn ike policy ike_policy1 remote-id ipv4_addr 11.0.1.1
set services ipsec-vpn traceoptions file ipsec_toby
set services ipsec-vpn traceoptions level all
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```

set interfaces ge-0/1/8 unit 0 family inet address 11.0.1.2/30
set interfaces ms-2/0/0 unit 0 family inet
set interfaces ms-2/0/0 unit 1 family inet
set interfaces ms-2/0/0 unit 1 service-domain inside
set interfaces ms-2/0/0 unit 2 family inet
set interfaces ms-2/0/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 80.0.0.1/24

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```

set routing-options static route 30.0.0.0/16 next-hop ms-2/0/0.1

```

```
[edit]
security-administrator@host:fips# exit
Exiting configuration mode
```

```
[edit]
security-administrator@host:fips> show services ipsec-vpn ike security-associations detail
```

```
IKE peer 11.0.1.1
  Role: Responder, State: Matured
  Initiator cookie: 80682e1b22e12f32, Responder cookie: 40c6c30301cfb1a3
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local gateway interface: ge-0/1/8.0
  Local: 11.0.1.2, Remote: 11.0.1.1
  Lifetime: Expires in 3289 seconds
  Peer ike-id: ipv4(any:0,[0..3]=11.0.1.1)
  Algorithms:
    Authentication      : hmac-sha256-128
    Encryption          : aes256-cbc
    Pseudo random function: hmac-sha256
    Diffie-Hellman group : 20
  Traffic statistics:
    Input  bytes :          1664
    Output bytes :          1641
    Input  packets:           2
    Output packets:           2
  Flags: IKE SA created
  IPSec security associations: 2 created, 0 deleted
```

```
[edit]
security-administrator@host:fips> show services ipsec-vpn ipsec security-associations
```

```
Service set: ss1, IKE Routing-instance: default
Rule: rule1, Term: term1, Tunnel index: 1
  Local gateway: 11.0.1.2, Remote gateway: 11.0.1.1
  IPSec inside interface: ms-2/0/0.1, Tunnel MTU: 1500
  UDP encapsulate: Disabled, UDP Destination port: 0
  Local identity: ipv4_subnet(any:0,[0..7]=80.0.0.0/16)
```

```

Remote identity: ipv4_subnet(any:0,[0..7]=30.0.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime:  0 days 0 hrs 5 mins 24 secs

Direction: inbound, SPI: 2267705568, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
Soft lifetime: Expires in 27625 seconds
Hard lifetime: Expires in 28476 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 1359811752, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
Soft lifetime: Expires in 27625 seconds
Hard lifetime: Expires in 28476 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

```

R2:

```

[edit]
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy1 local-id ipv4_addr 11.0.1.1
security-administrator@host:fips# set services ipsec-vpn ike policy ike_policy1 remote-id ipv4_addr 11.0.1.2
security-administrator@host:fips# commit
commit complete

```

```

[edit]
security-administrator@host:fips# show services | display set

```

```

set services service-set ssl next-hop-service inside-service-interface
ms-2/0/0.1
set services service-set ssl next-hop-service outside-service-interface
ms-2/0/0.2
set services service-set ssl ipsec-vpn-options local-gateway 11.0.1.1
set services service-set ssl ipsec-vpn-rules rule1
set services ipsec-vpn rule rule1 term term1 from source-address 30.0.0.0/16
set services ipsec-vpn rule rule1 term term1 from destination-address
80.0.0.0/16
set services ipsec-vpn rule rule1 term term1 then remote-gateway 11.0.1.2
set services ipsec-vpn rule rule1 term term1 then dynamic ike-policy
ike_policy1
set services ipsec-vpn rule rule1 term term1 then dynamic ipsec-policy
ipsec_policy1
set services ipsec-vpn rule rule1 term term1 then anti-replay-window-size
4096
set services ipsec-vpn rule rule1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy1 perfect-forward-secrecy
keys group20
set services ipsec-vpn ipsec policy ipsec_policy1 proposals ipsec_proposal1
set services ipsec-vpn ike proposal ike_proposal1 authentication-method
rsa-signatures
set services ipsec-vpn ike proposal ike_proposal1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal1 authentication-algorithm
sha-256
set services ipsec-vpn ike proposal ike_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ike policy ike_policy1 version 2
set services ipsec-vpn ike policy ike_policy1 proposals ike_proposal1
set services ipsec-vpn ike policy ike_policy1 local-id ipv4_addr 11.0.1.1
set services ipsec-vpn ike policy ike_policy1 local-certificate r0_cert_id
set services ipsec-vpn ike policy ike_policy1 remote-id ipv4_addr 11.0.1.2
set services ipsec-vpn traceoptions file ipsec_toby
set services ipsec-vpn traceoptions level all
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```
set interfaces ge-0/1/3 unit 0 family inet address 11.0.1.1/30
set interfaces ms-2/0/0 unit 0 family inet
set interfaces ms-2/0/0 unit 1 family inet
set interfaces ms-2/0/0 unit 1 service-domain inside
set interfaces ms-2/0/0 unit 2 family inet
set interfaces ms-2/0/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 30.0.0.1/24
```

[edit]

security-administrator@host:fips# **show routing-options | display set**

```
set routing-options static route 80.0.0.0/16 next-hop ms-2/0/0.1
```

[edit]

security-administrator@host:fips# **exit**

Exiting configuration mode

[edit]

security-administrator@host:fips> **show services ipsec-vpn ike security-associations detail**

```
IKE peer 11.0.1.2
  Role: Initiator, State: Matured
  Initiator cookie: 80682e1b22e12f32, Responder cookie: 40c6c30301cfbla3
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local gateway interface: ge-0/1/3.0
  Local: 11.0.1.1, Remote: 11.0.1.2
  Lifetime: Expires in 3267 seconds
  Peer ike-id: ipv4(any:0,[0..3]=11.0.1.2)
  Algorithms:
    Authentication      : hmac-sha256-128
    Encryption          : aes256-cbc
```



```

Pseudo random function: hmac-sha256
Diffie-Hellman group   : 20
Traffic statistics:
Input  bytes   :          1641
Output bytes   :          1664
Input  packets :           2
Output packets :           2
Flags: IKE SA created
IPSec security associations: 2 created, 0 deleted

```

[edit]

security-administrator@host:fps> **show services ipsec-vpn ipsec security-associations detail**

```

Service set: ssl, IKE Routing-instance: default
Rule: rule1, Term: term1, Tunnel index: 1
Local gateway: 11.0.1.1, Remote gateway: 11.0.1.2
IPSec inside interface: ms-2/0/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
Local identity: ipv4_subnet(any:0,[0..7]=30.0.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=80.0.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime:  0 days 0 hrs 5 mins 44 secs

Direction: inbound, SPI: 1359811752, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
Soft lifetime: Expires in 27650 seconds
Hard lifetime: Expires in 28456 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 2267705568, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc

```

```
(256 bits)
  Soft lifetime: Expires in 27650 seconds
  Hard lifetime: Expires in 28456 seconds
  Anti-replay service: Enabled, Replay window size: 4096
  Copy ToS: Enabled
  Copy TTL: Disabled, TTL value: 64
  SA lifetime: 28800 seconds
```

Sample IPsec VPN Configuration with FQDN as Reference Identifier

R2:

[edit]

security-administrator@host:fips# **show services | display set**

```
set services service-set ssl next-hop-service inside-service-interface
ms-2/0/0.1
set services service-set ssl next-hop-service outside-service-interface
ms-2/0/0.2
set services service-set ssl ipsec-vpn-options local-gateway 11.0.1.2
set services service-set ssl ipsec-vpn-rules rule1
set services ipsec-vpn rule rule1 term term1 from source-address 80.0.0.0/16
set services ipsec-vpn rule rule1 term term1 from destination-address
30.0.0.0/16
set services ipsec-vpn rule rule1 term term1 then remote-gateway 11.0.1.1
set services ipsec-vpn rule rule1 term term1 then dynamic ike-policy
ike_policy1
set services ipsec-vpn rule rule1 term term1 then dynamic ipsec-policy
ipsec_policy1
set services ipsec-vpn rule rule1 term term1 then anti-replay-window-size
4096
set services ipsec-vpn rule rule1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal1 encryption-algorithm
aes-256-cbc
```

```

set services ipsec-vpn ipsec policy ipsec_policy1 perfect-forward-secrecy
keys group20
set services ipsec-vpn ipsec policy ipsec_policy1 proposals ipsec_proposal1
set services ipsec-vpn ike proposal ike_proposal1 authentication-method
ecdsa-signatures-256
set services ipsec-vpn ike proposal ike_proposal1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal1 authentication-algorithm
sha-256
set services ipsec-vpn ike proposal ike_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ike policy ike_policy1 version 2
set services ipsec-vpn ike policy ike_policy1 proposals ike_proposal1
set services ipsec-vpn ike policy ike_policy1 local-id fqdn
R2.englab.juniper.net
set services ipsec-vpn ike policy ike_policy1 local-certificate r1_cert_id
set services ipsec-vpn ike policy ike_policy1 remote-id fqdn
R0.englab.juniper.net
set services ipsec-vpn traceoptions file ipsec_toby
set services ipsec-vpn traceoptions level all
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```

set interfaces ge-0/1/8 unit 0 family inet address 11.0.1.2/30
set interfaces ms-2/0/0 unit 0 family inet
set interfaces ms-2/0/0 unit 1 family inet
set interfaces ms-2/0/0 unit 1 service-domain inside
set interfaces ms-2/0/0 unit 2 family inet
set interfaces ms-2/0/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 80.0.0.1/24

```

[edit]

security-administrator@host:fips# **show routing-options | display set**

```
set routing-options static route 30.0.0.0/16 next-hop ms-2/0/0.1
```

[edit]

security-administrator@host:fips# **show security | display set**

```
set security pki ca-profile ca_profile1 ca-identity ca_profile1_id
```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ike security-associations detail**

```
IKE peer 11.0.1.1
Role: Responder, State: Matured
  Initiator cookie: 0f81b5e9elc9b88a, Responder cookie: fad59006894eb4d7
  Exchange type: IKEv2, Authentication method: ECDSA-signatures (256 bit
key)
  Local gateway interface: ge-0/1/8.0
  Local: 11.0.1.2, Remote: 11.0.1.1
  Lifetime: Expires in 3599 seconds
  Peer ike-id: fqdn(any:0,[0..23]=R0.englab.juniper.net)
  Algorithms:
    Authentication      : hmac-sha256-128
    Encryption          : aes256-cbc
    Pseudo random function: hmac-sha256
    Diffie-Hellman group : 20
  Traffic statistics:
    Input  bytes  :          1152
    Output bytes  :          1097
    Input  packets:           2
    Output packets:           2
  Flags: IKE SA created
  IPSec security associations: 2 created, 0 deleted
```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ipsec security-associations detail**

```
Service set: ssl, IKE Routing-instance: default
Rule: rule1, Term: term1, Tunnel index: 1
Local gateway: 11.0.1.2, Remote gateway: 11.0.1.1
IPSec inside interface: ms-2/0/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
Local identity: ipv4_subnet(any:0,[0..7]=80.0.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=30.0.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime: 0 days 0 hrs 0 mins 14 secs

Direction: inbound, SPI: 1648581290, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
Soft lifetime: Expires in 27971 seconds
Hard lifetime: Expires in 28786 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 3998160043, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
Soft lifetime: Expires in 27971 seconds
Hard lifetime: Expires in 28786 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds
```

DUT:

[edit]

security-administrator@host:fips# **show services | display set**

```

set services service-set ssl next-hop-service inside-service-interface
ms-2/0/0.1
set services service-set ssl next-hop-service outside-service-interface
ms-2/0/0.2
set services service-set ssl ipsec-vpn-options local-gateway 11.0.1.1
set services service-set ssl ipsec-vpn-rules rule1
set services ipsec-vpn rule rule1 term term1 from source-address 30.0.0.0/16
set services ipsec-vpn rule rule1 term term1 from destination-address
80.0.0.0/16
set services ipsec-vpn rule rule1 term term1 then remote-gateway 11.0.1.2
set services ipsec-vpn rule rule1 term term1 then dynamic ike-policy
ike_policy1
set services ipsec-vpn rule rule1 term term1 then dynamic ipsec-policy
ipsec_policy1
set services ipsec-vpn rule rule1 term term1 then anti-replay-window-size
4096
set services ipsec-vpn rule rule1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy1 perfect-forward-secrecy
keys group20
set services ipsec-vpn ipsec policy ipsec_policy1 proposals ipsec_proposal1
set services ipsec-vpn ike proposal ike_proposal1 authentication-method
ecdsa-signatures-256
set services ipsec-vpn ike proposal ike_proposal1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal1 authentication-algorithm
sha-256
set services ipsec-vpn ike proposal ike_proposal1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ike policy ike_policy1 version 2
set services ipsec-vpn ike policy ike_policy1 proposals ike_proposal1
set services ipsec-vpn ike policy ike_policy1 local-id fqdn
R0.englab.juniper.net
set services ipsec-vpn ike policy ike_policy1 local-certificate r0_cert_id
set services ipsec-vpn ike policy ike_policy1 remote-id fqdn
R2.englab.juniper.net
set services ipsec-vpn traceoptions file ipsec_toby
set services ipsec-vpn traceoptions level all

```

```
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately
```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```
set interfaces ge-0/1/3 unit 0 family inet address 11.0.1.1/30
set interfaces ms-2/0/0 unit 0 family inet
set interfaces ms-2/0/0 unit 1 family inet
set interfaces ms-2/0/0 unit 1 service-domain inside
set interfaces ms-2/0/0 unit 2 family inet
set interfaces ms-2/0/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 30.0.0.1/24
```

[edit]

security-administrator@host:fips# **show routing-options | display set**

```
set routing-options static route 80.0.0.0/16 next-hop ms-2/0/0.1
```

[edit]

security-administrator@host:fips# **show security | display set**

```
set security pki ca-profile ca_profile1 ca-identity ca_profile1_id
```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ike security-associations detail**

```

IKE peer 11.0.1.2
Role: Initiator, State: Matured
Initiator cookie: 0f81b5e9e1c9b88a, Responder cookie: fad59006894eb4d7
Exchange type: IKEv2, Authentication method: ECDSA-signatures (256 bit
key)
Local gateway interface: ge-0/1/3.0
Local: 11.0.1.1, Remote: 11.0.1.2
Lifetime: Expires in 3574 seconds
Peer ike-id: fqdn(any:0,[0..22]=R2.englab.juniper.net)
Algorithms:
  Authentication      : hmac-sha256-128
  Encryption          : aes256-cbc
  Pseudo random function: hmac-sha256
  Diffie-Hellman group : 20
Traffic statistics:
  Input  bytes :          1097
  Output bytes :          1152
  Input  packets:           2
  Output packets:           2
Flags: IKE SA created
IPSec security associations: 2 created, 0 deleted

```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ipsec security-associations detail**

```

Service set: ssl, IKE Routing-instance: default
  Rule: rule1, Term: term1, Tunnel index: 1
Local gateway: 11.0.1.1, Remote gateway: 11.0.1.2
IPSec inside interface: ms-2/0/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
Local identity: ipv4_subnet(any:0,[0..7]=30.0.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=80.0.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime:  0 days 0 hrs 0 mins 33 secs

Direction: inbound, SPI: 3998160043, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed

```



```

    Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
    Soft lifetime: Expires in 27905 seconds
    Hard lifetime: Expires in 28767 seconds
    Anti-replay service: Enabled, Replay window size: 4096
    Copy ToS: Enabled
    Copy TTL: Disabled, TTL value: 64
    SA lifetime: 28800 seconds

    Direction: outbound, SPI: 1648581290, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-cbc
(256 bits)
    Soft lifetime: Expires in 27905 seconds
    Hard lifetime: Expires in 28767 seconds
    Anti-replay service: Enabled, Replay window size: 4096
    Copy ToS: Enabled
    Copy TTL: Disabled, TTL value: 64
    SA lifetime: 28800 seconds

```

[edit]

security-administrator@host:fips# run ping 80.0.0.1 source 30.0.0.1

```

    PING 80.0.0.1 (80.0.0.1): 56 data bytes
64 bytes from 80.0.0.1: icmp_seq=0 ttl=64 time=1.717 ms
64 bytes from 80.0.0.1: icmp_seq=1 ttl=64 time=0.994 ms
^C
--- 80.0.0.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.994/1.356/1.717/0.361 ms

```

Sample Configuration for Distinguished Name as Reference Identifier

DUT:

[edit]

security-administrator@host:fips# **show services | display set**

```

set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
inside-service-interface ms-2/1/0.1
set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
outside-service-interface ms-2/1/0.2
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-options local-gateway
20.0.0.1
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-rules
vpn_rule_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
source-address 10.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
destination-address 30.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
remote-gateway 20.0.0.2
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ike-policy ike_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ipsec-policy ipsec_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1 protocol
esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1
perfect-forward-secrecy keys group20
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1 proposals
ipsec_proposal_ms_2_1_0_1
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
authentication-method rsa-signatures
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 version 2
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 proposals
ike_proposal_ms_2_1_0_1

```

```

set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 local-id
distinguished-name
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 local-certificate
juniperb
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 remote-id
distinguished-name wilddcard CN=juniperA
set services ipsec-vpn traceoptions file ipsec_fw_log1
set services ipsec-vpn traceoptions level all
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```

set interfaces ge-0/0/2 unit 0 family inet address 10.1.0.2/24
set interfaces ge-0/1/3 unit 0 family inet address 20.0.0.1/30
set interfaces ms-2/1/0 unit 0 family inet
set interfaces ms-2/1/0 unit 1 family inet
set interfaces ms-2/1/0 unit 1 family inet6
set interfaces ms-2/1/0 unit 1 service-domain inside
set interfaces ms-2/1/0 unit 2 family inet
set interfaces ms-2/1/0 unit 2 family inet6
set interfaces ms-2/1/0 unit 2 service-domain outside

```

[edit]

security-administrator@host:fips# **show routing-options | display set**

```

set routing-options static route 30.1.0.0/16 next-hop ms-2/1/0.1

```

[edit]

security-administrator@host:fips# **show security | display set**

```
set security pki ca-profile root ca-identity root
```

[edit]

```
security-administrator@host:fips# run show security pki local-certificate certificate-id juniperb detail
```

```
Certificate identifier: juniperb
Certificate version: 3
Serial number: 0000000a
Issuer:
  Common name: juniperCA
Subject:
  Country: US, State: MD, Common name: juniperB
Subject string:
  C=US, ST=MD, CN=juniperB
Validity:
  Not before: 02-26-2019 17:22 UTC
  Not after: 02-24-2020 19:20 UTC
Public key algorithm: rsaEncryption(2048 bits)
30:82:01:0a:02:82:01:01:00:d1:e2:09:34:d0:e2:a8:e8:1d:eb:9d
7e:1c:62:f4:b5:ac:3d:1a:ab:9c:13:e6:bf:3d:7a:06:19:2a:1d:11
83:28:6d:15:73:ff:b7:ea:3d:50:76:99:e0:a4:fa:82:2b:42:3e:71
3c:96:45:70:70:d1:76:fd:79:79:df:c0:e5:ce:87:8b:80:82:15:af
01:23:b6:76:8b:28:98:41:c4:6a:f9:0d:3b:b4:f8:f9:0f:0c:3c:d5
94:39:25:1b:69:d8:e5:80:83:35:57:3d:f0:92:be:10:1f:19:8a:69
61:dd:a3:cd:98:bd:df:87:df:70:30:3d:ab:2a:24:a2:9b:e6:92:72
a7:0a:fc:b4:4c:8a:29:c3:cb:13:89:85:53:a9:5e:44:80:1c:7f:25
57:13:2f:de:ce:d4:f4:38:ed:3e:a1:e6:a9:10:29:13:33:07:47:fb
72:84:f8:f0:e4:a4:30:ca:c1:ec:cc:75:16:66:79:89:18:a1:13:e9
dc:3a:13:c9:96:b5:0c:3b:6c:18:02:b3:0b:86:09:f2:8c:e6:64:ea
7a:d6:43:f2:29:9d:a3:00:10:f8:10:c1:f7:31:ef:50:d9:a8:03:d5
58:78:b2:83:fc:eb:f2:7a:20:3c:9b:82:03:7b:20:43:51:73:41:7b
1d:f1:21:ca:fd:02:03:01:00:01
Signature algorithm: sha256WithRSAEncryption
Use for key: Data encipherment, Key encipherment, Non repudiation, Digital
signature
Fingerprint:
  29:69:17:76:92:f4:68:9d:20:d2:04:6e:38:2e:e5:77:42:71:ad:f9 (sha1)
```

```

Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

[edit]

security-administrator@host:fps# **run show security pki ca-certificate ca-profile root detail**

```

Certificate identifier: root
  Certificate version: 3
  Serial number: 00000001
  Issuer:
    Common name: juniperCA
  Subject:
    Common name: juniperCA
  Subject string:
    CN=juniperCA
  Validity:
    Not before: 02-24-2019 19:20 UTC
    Not after: 02-24-2020 19:20 UTC
  Public key algorithm: rsaEncryption(2048 bits)
    30:82:01:0a:02:82:01:01:00:d1:e2:09:34:d0:e2:a8:e8:1d:eb:9d
    7e:1c:62:f4:b5:ac:3d:1a:ab:9c:13:e6:bf:3d:7a:06:19:2a:1d:11
    83:28:6d:15:73:ff:b7:ea:3d:50:76:99:e0:a4:fa:82:2b:42:3e:71
    3c:96:45:70:70:d1:76:fd:79:79:df:c0:e5:ce:87:8b:80:82:15:af
    01:23:b6:76:8b:28:98:41:c4:6a:f9:0d:3b:b4:f8:f9:0f:0c:3c:d5
    94:39:25:1b:69:d8:e5:80:83:35:57:3d:f0:92:be:10:1f:19:8a:69
    61:dd:a3:cd:98:bd:df:87:df:70:30:3d:ab:2a:24:a2:9b:e6:92:72
    a7:0a:fc:b4:4c:8a:29:c3:cb:13:89:85:53:a9:5e:44:80:1c:7f:25
    57:13:2f:de:ce:d4:f4:38:ed:3e:a1:e6:a9:10:29:13:33:07:47:fb
    72:84:f8:f0:e4:a4:30:ca:c1:ec:cc:75:16:66:79:89:18:a1:13:e9
    dc:3a:13:c9:96:b5:0c:3b:6c:18:02:b3:0b:86:09:f2:8c:e6:64:ea
    7a:d6:43:f2:29:9d:a3:00:10:f8:10:c1:f7:31:ef:50:d9:a8:03:d5
    58:78:b2:83:fc:eb:f2:7a:20:3c:9b:82:03:7b:20:43:51:73:41:7b
    1d:f1:21:ca:fd:02:03:01:00:01
  Signature algorithm: sha256WithRSAEncryption
  Use for key: CRL signing, Certificate signing

```

Fingerprint:

9b:22:63:46:32:6f:f0:1c:fe:37:5f:eb:59:bb:8d:87:05:d3:b1:a6 (sha1)

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ike security-associations detail**

```
IKE peer 20.0.0.2
Role: Initiator, State: Matured
Initiator cookie: 7b7229d8e0d058d6, Responder cookie: ad14892b16f0ec47
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 20.0.0.1, Remote: 20.0.0.2
Lifetime: Expires in 2885 seconds
Peer ike-id: der_asn1_dn(any:0,[0..46]=C=US, ST=MD, CN=juniperA)
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : aes256-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : 20
Traffic statistics:
  Input  bytes : 0
  Output bytes : 0
  Input  packets: 0
  Output packets: 0
Flags: IKE SA created
IPSec security associations: 0 created, 0 deleted
```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ipsec security-associations detail**

```
Service set: ipsec_ss_ms_2_1_0_1, IKE Routing-instance: default
Rule: vpn_rule_ms_2_1_0_1, Term: term1, Tunnel index: 1
Local gateway: 20.0.0.1, Remote gateway: 20.0.0.2
IPSec inside interface: ms-2/1/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
```

```

Local identity: ipv4_subnet(any:0,[0..7]=10.1.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=30.1.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime:  0 days 0 hrs 55 mins 37 secs

Direction: inbound, SPI: 2743594902, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Soft lifetime: Expires in 24470 seconds
Hard lifetime: Expires in 25463 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 779717468, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Soft lifetime: Expires in 24470 seconds
Hard lifetime: Expires in 25463 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

```

R2:

[edit]

security-administrator@host:fips# **show services | display set**

```

set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
inside-service-interface ms-2/1/0.1
set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
outside-service-interface ms-2/1/0.2
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-options local-gateway

```

```

20.0.0.2
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-rules
vpn_rule_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
source-address 30.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
destination-address 10.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
remote-gateway 20.0.0.1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ike-policy ike_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ipsec-policy ipsec_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1 protocol
esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1
perfect-forward-secrecy keys group20
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1 proposals
ipsec_proposal_ms_2_1_0_1
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
authentication-method rsa-signatures
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 version 2
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 proposals
ike_proposal_ms_2_1_0_1
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 local-id
distinguished-name
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 local-certificate
junipera
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 remote-id
distinguished-name wildcard CN=juniperB
set services ipsec-vpn traceoptions file ipsec_fw_log1

```



```

set services ipsec-vpn traceoptions level all
set services ipsec-vpn traceoptions flag all
set services ipsec-vpn establish-tunnels immediately

```

[edit]

security-administrator@host:fips# **show interfaces | display set**

```

set interfaces ge-0/1/7 unit 0 family inet address 30.1.0.2/24
set interfaces ge-0/1/8 unit 0 family inet address 20.0.0.2/30
set interfaces ms-2/1/0 unit 0 family inet
set interfaces ms-2/1/0 unit 1 family inet
set interfaces ms-2/1/0 unit 1 family inet6
set interfaces ms-2/1/0 unit 1 service-domain inside
set interfaces ms-2/1/0 unit 2 family inet
set interfaces ms-2/1/0 unit 2 family inet6
set interfaces ms-2/1/0 unit 2 service-domain outside

```

[edit]

security-administrator@host:fips# **show routing-options | display set**

```

set routing-options static route 10.1.0.0/16 next-hop ms-2/1/0.1

```

[edit]

security-administrator@host:fips# **show security | display set**

```

set security pki ca-profile root ca-identity root

```

[edit]

```
security-administrator@host:fips# run show security pki local-certificate certificate-id junipera detail
```

```
Certificate identifier: junipera
Certificate version: 3
Serial number: 00000009
Issuer:
  Common name: juniperCA
Subject:
  Country: US, State: MD, Common name: juniperA
Subject string:
  C=US, ST=MD, CN=juniperA
Validity:
  Not before: 02-26-2019 17:21 UTC
  Not after: 02-24-2020 19:20 UTC
Public key algorithm: rsaEncryption(2048 bits)
  30:82:01:0a:02:82:01:01:00:d1:e2:09:34:d0:e2:a8:e8:1d:eb:9d
  7e:1c:62:f4:b5:ac:3d:1a:ab:9c:13:e6:bf:3d:7a:06:19:2a:1d:11
  83:28:6d:15:73:ff:b7:ea:3d:50:76:99:e0:a4:fa:82:2b:42:3e:71
  3c:96:45:70:70:d1:76:fd:79:79:df:c0:e5:ce:87:8b:80:82:15:af
  01:23:b6:76:8b:28:98:41:c4:6a:f9:0d:3b:b4:f8:f9:0f:0c:3c:d5
  94:39:25:1b:69:d8:e5:80:83:35:57:3d:f0:92:be:10:1f:19:8a:69
  61:dd:a3:cd:98:bd:df:87:df:70:30:3d:ab:2a:24:a2:9b:e6:92:72
  a7:0a:fc:b4:4c:8a:29:c3:cb:13:89:85:53:a9:5e:44:80:1c:7f:25
  57:13:2f:de:ce:d4:f4:38:ed:3e:a1:e6:a9:10:29:13:33:07:47:fb
  72:84:f8:f0:e4:a4:30:ca:c1:ec:cc:75:16:66:79:89:18:a1:13:e9
  dc:3a:13:c9:96:b5:0c:3b:6c:18:02:b3:0b:86:09:f2:8c:e6:64:ea
  7a:d6:43:f2:29:9d:a3:00:10:f8:10:c1:f7:31:ef:50:d9:a8:03:d5
  58:78:b2:83:fc:eb:f2:7a:20:3c:9b:82:03:7b:20:43:51:73:41:7b
  1d:f1:21:ca:fd:02:03:01:00:01
Signature algorithm: sha256WithRSAEncryption
Use for key: Data encipherment, Key encipherment, Non repudiation, Digital
signature
Fingerprint:
  b2:49:38:a0:c9:2b:33:17:8a:33:97:91:e4:93:41:af:20:9f:4c:86 (sha1)
Auto-re-enrollment:
  Status: Disabled
```

[edit]

```
security-administrator@host:fips# run show services ipsec-vpn ike security-associations detail
```

```

IKE peer 20.0.0.1
  Role: Responder, State: Matured
  Initiator cookie: 7b7229d8e0d058d6, Responder cookie: ad14892b16f0ec47
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local: 20.0.0.2, Remote: 20.0.0.1
  Lifetime: Expires in 3415 seconds
  Peer ike-id: der_asn1_dn(any:0,[0..46]=C=US, ST=MD, CN=juniperB)
  Algorithms:
    Authentication      : hmac-sha1-96
    Encryption          : aes256-cbc
    Pseudo random function: hmac-sha1
    Diffie-Hellman group  : 20
  Traffic statistics:
    Input  bytes  : 0
    Output bytes  : 0
    Input  packets: 0
    Output packets: 0
  Flags: IKE SA created
  IPSec security associations: 0 created, 0 deleted

```

[edit]

security-administrator@host:fips# **run show services ipsec-vpn ipsec security-associations detail**

```

Service set: ipsec_ss_ms_2_1_0_1, IKE Routing-instance: default

Rule: vpn_rule_ms_2_1_0_1, Term: term1, Tunnel index: 1
Local gateway: 20.0.0.2, Remote gateway: 20.0.0.1
IPSec inside interface: ms-2/1/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
Local identity: ipv4_subnet(any:0,[0..7]=30.1.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.0.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime:  0 days 0 hrs 46 mins 38 secs

Direction: inbound, SPI: 779717468, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

```

```

Soft lifetime: Expires in 25054 seconds
Hard lifetime: Expires in 26002 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 2743594902, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Soft lifetime: Expires in 25054 seconds
Hard lifetime: Expires in 26002 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

```

Generating Certificate Signing Request (CSR)

Sample commands for generating key-pair and CSR:

```
security-administrator@host:fips> request security pki generate-key-pair type ecdsa size 256 certificate-id
r1_cert_id
```

```
Generated key pair r1_cert_id, key size 256 bits
```

```
security-administrator@host:fips> request security pki generate-certificate-request certificate-id r1_cert_id
filename subject CN=11.0.1.2 email router@juniper.net /var/tmp/11.0.1.2.csr
```

```

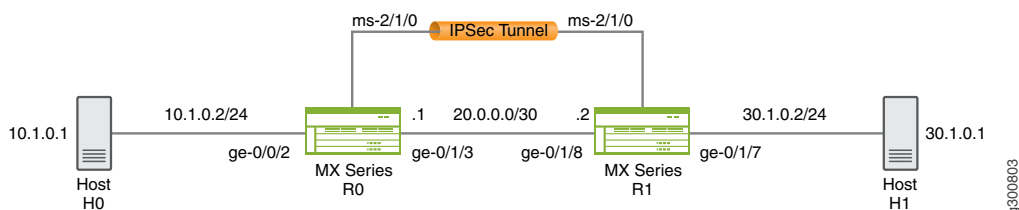
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBAjCBpwIBADATMREwDwYDVQQDEwgxMS4wLjEuMjBZMBMGBYqGSM49AgEGCCqG
SM49AwEHA0IABLRebeXGFF+AnH6I0AQu8gFQwOCbAm89wazpUpQs5RIGiVfYGgV1
xrwTGcQoKYc+a8PqJ7EQcffSttdQ1fUG9KqgMjAwBgkqhkiG9w0BCQ4xIzAhMB8G
AlUdEQQYMBaBFCJiYWxhamlAanVuaXBldi5uZXQiMAwGCCqGSM49BAMCBQADSAAw
RQIgKbEsYSH8QE4ZKo97z3jDwIWutr2pOp4H42jTvqONL+kCIQChgA/if9TcflyA
yrX/0duSsUHi/tcOeP+RxWdAgpb6dA==
-----END CERTIFICATE REQUEST-----

```

For more information, refer https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/request-security-pki-generate-certificate-request.html.

Configuring Firewall Rules

MX devices allow configuring firewall filter to allow or reject specific traffic.



The following procedures explain how to configure IPsec VPN and firewall rules:

1. Configure IPsec VPN between R0-R1.

R0:

```

[edit]
security-administrator@host:fips# show services | display set

set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
inside-service-interface ms-2/1/0.1
set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
outside-service-interface ms-2/1/0.2

```

```

set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-options local-gateway
  20.0.0.1
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-rules vpn_rule_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from source-address
  10.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
destination-address 30.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then remote-gateway
  20.0.0.2
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ike-policy ike_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ipsec-policy ipsec_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1
perfect-forward-secrecy keys group20
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1 proposals
ipsec_proposal_ms_2_1_0_1
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 encryption-algorithm
  aes-256-cbc
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 version 2
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 proposals
ike_proposal_ms_2_1_0_1

```

[edit]

security-administrator@host:fips# **prompt services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 pre-shared-key**
ascii-text

New ascii-text (secret):

Retype new ascii-text (secret):

```
[edit]
security-administrator@host:fips# set services ipsec-vpn traceoptions file ipsec_fw_log1
security-administrator@host:fips# set services ipsec-vpn traceoptions level all
security-administrator@host:fips# set services ipsec-vpn traceoptions flag all
security-administrator@host:fips# set services ipsec-vpn establish-tunnels immediately
```

```
[edit]
security-administrator@host:fips# show interfaces | display set
```

```
set interfaces ge-0/0/2 unit 0 family inet address 10.1.0.2/24
set interfaces ge-0/1/3 unit 0 family inet address 20.0.0.1/30
set interfaces ms-2/1/0 unit 0 family inet
set interfaces ms-2/1/0 unit 1 family inet
set interfaces ms-2/1/0 unit 1 family inet6
set interfaces ms-2/1/0 unit 1 service-domain inside
set interfaces ms-2/1/0 unit 2 family inet
set interfaces ms-2/1/0 unit 2 family inet6
set interfaces ms-2/1/0 unit 2 service-domain outside
```

```
[edit]
security-administrator@host:fips# show routing-options | display set
```

```
set routing-options static route 30.1.0.0/16 next-hop ms-2/1/0.1
```

R1:

```
[edit]
security-administrator@host:fips# show services | display set

set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
inside-service-interface ms-2/1/0.1
set services service-set ipsec_ss_ms_2_1_0_1 next-hop-service
outside-service-interface ms-2/1/0.2
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-options local-gateway
20.0.0.2
set services service-set ipsec_ss_ms_2_1_0_1 ipsec-vpn-rules vpn_rule_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from source-address
```

```

30.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 from
destination-address 10.1.0.0/16
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then remote-gateway
20.0.0.1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ike-policy ike_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then dynamic
ipsec-policy ipsec_policy_ms_2_1_0_1
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 term term1 then
anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_2_1_0_1 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
authentication-algorithm hmac-sha-256-128
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_2_1_0_1
encryption-algorithm aes-256-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1
perfect-forward-secrecy keys group20
set services ipsec-vpn ipsec policy ipsec_policy_ms_2_1_0_1 proposals
ipsec_proposal_ms_2_1_0_1
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1
authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 dh-group group20
set services ipsec-vpn ike proposal ike_proposal_ms_2_1_0_1 encryption-algorithm
aes-256-cbc
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 version 2
set services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 proposals
ike_proposal_ms_2_1_0_1

```

[edit]

security-administrator@host:fips# **prompt services ipsec-vpn ike policy ike_policy_ms_2_1_0_1 pre-shared-key**
ascii-text

New ascii-text (secret):

Retype new ascii-text (secret):

[edit]

security-administrator@host:fips# **set services ipsec-vpn traceoptions file ipsec_fw_log1**
security-administrator@host:fips# **set services ipsec-vpn traceoptions level all**
security-administrator@host:fips# **set services ipsec-vpn traceoptions flag all**


```
security-administrator@host:fips# set services ipsec-vpn establish-tunnels immediately
```

```
[edit]
```

```
security-administrator@host:fips# show interfaces | display set
```

```
set interfaces ge-0/1/8 unit 0 family inet address 20.0.0.2/30
set interfaces ge-0/1/7 unit 0 family inet address 30.1.0.2/24
set interfaces ms-2/1/0 unit 0 family inet
set interfaces ms-2/1/0 unit 1 family inet
set interfaces ms-2/1/0 unit 1 family inet6
set interfaces ms-2/1/0 unit 1 service-domain inside
set interfaces ms-2/1/0 unit 2 family inet
set interfaces ms-2/1/0 unit 2 family inet6
set interfaces ms-2/1/0 unit 2 service-domain outside
```

```
[edit]
```

```
security-administrator@host:fips# show routing-options | display set
```

```
set routing-options static route 10.1.0.0/16 next-hop ms-2/1/0.1
```

2. Configure firewall rule.

Enable firewall filter to allow traffic from specific source and destination addresses and reject all other traffic. For example, the first rule term 1 allows traffic from source-address 30.1.0.1/32 to communicate with only 10.1.0.1/32 address. The second rule rejects all other traffic.

```
[edit]
```

```
security-administrator@host:fips# show firewall | display set
```

```
set firewall family inet filter fw_filter1 term 1 from source-address 30.1.0.1/32
set firewall family inet filter fw_filter1 term 1 from destination-address
10.1.0.1/32
set firewall family inet filter fw_filter1 term 1 then count inc1
set firewall family inet filter fw_filter1 term 1 then log
set firewall family inet filter fw_filter1 term 1 then accept
set firewall family inet filter fw_filter1 term 2 then count inc2
set firewall family inet filter fw_filter1 term 2 then log
```

```
set firewall family inet filter fw_filter1 term 2 then reject
set firewall traceoptions file firewall_log
set firewall traceoptions file size 1g
set firewall traceoptions file world-readable
set firewall traceoptions flag all
```

NOTE: The firewall rules are processed in the order they are configured.

3. Apply input firewall filter on R0 router MS-MPC interface.

```
[edit]
security-administrator@host:fips# set interfaces ms-2/1/0 unit 1 family inet filter input fw_filter1
```

4. Send traffic from H1 to H0 and monitor firewall logs based on accept or reject rule.

Accepted traffic logs on R0:

```
[edit]
security-administrator@host:fips# run show firewall log
```

```
Log :
Time      Filter  Action Interface  Protocol  Src Addr  Dest Addr
20:39:20  pfe        A      ms-2/1/0.1  ICMP     30.1.0.1  10.1.0.1
20:39:19  pfe        A      ms-2/1/0.1  ICMP     30.1.0.1  10.1.0.1
20:39:18  pfe        A      ms-2/1/0.1  ICMP     30.1.0.1  10.1.0.1
```

Rejected traffic logs on R0:

```
[edit]
security-administrator@host:fips# run show firewall log
```

```
Log :
```

Time	Filter	Action	Interface	Protocol	Src Addr	Dest Addr
20:43:20	pfe	R	ms-2/1/0.1	ICMP	30.1.0.5	10.1.0.1
20:43:19	pfe	R	ms-2/1/0.1	ICMP	30.1.0.5	10.1.0.1
20:43:18	pfe	R	ms-2/1/0.1	ICMP	30.1.0.5	10.1.0.1

9

CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 133

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that the Juniper Networks Junos operating system (Junos OS) in FIPS mode meets the security requirements of FIPS 140-2 Level 1. To validate the output of cryptographic algorithms approved for FIPS and test the integrity of some system modules, the router 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_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **xlp_kats**—KAT for MS-MPC line card

The KAT self-tests are performed automatically at startup. 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.

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

For MX Series routers with RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G:

```
user@host> file show /var/log/messages
```

```

    mgd: Running FIPS Self-tests
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-KEYWRAP 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 OpenSSL KATS:
mgd:   FIPS RNG Known Answer Test:                 Passed
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: 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:   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:

```

For MX Series routers with MS-MPC:

user@host> **file show /var/log/messages**

```

Testing jsf crypto (mpc xlp platform):
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...

```

station 281, testing SAE engine no. 11 ...

DES3-CBC Known Answer Test:

Passed

station 281, testing SAE engine no. 0 ...

station 281, testing SAE engine no. 4 ...

station 281, testing SAE engine no. 8 ...

station 281, testing SAE engine no. 1 ...

station 281, testing SAE engine no. 5 ...

station 281, testing SAE engine no. 9 ...

station 281, testing SAE engine no. 2 ...

station 281, testing SAE engine no. 6 ...

station 281, testing SAE engine no. 10 ...

station 281, testing SAE engine no. 3 ...

station 281, testing SAE engine no. 7 ...

station 281, testing SAE engine no. 11 ...

HMAC-SHA2-256 Known Answer Test:

Passed

station 281, testing SAE engine no. 0 ...

station 281, testing SAE engine no. 4 ...

station 281, testing SAE engine no. 8 ...

station 281, testing SAE engine no. 1 ...

station 281, testing SAE engine no. 5 ...

station 281, testing SAE engine no. 9 ...

station 281, testing SAE engine no. 2 ...

station 281, testing SAE engine no. 6 ...

station 281, testing SAE engine no. 10 ...

station 281, testing SAE engine no. 3 ...

station 281, testing SAE engine no. 7 ...

station 281, testing SAE engine no. 11 ...

station 281, testing SAE engine no. 0 ...

station 281, testing SAE engine no. 4 ...

station 281, testing SAE engine no. 8 ...

station 281, testing SAE engine no. 1 ...

station 281, testing SAE engine no. 5 ...

station 281, testing SAE engine no. 9 ...

station 281, testing SAE engine no. 2 ...

station 281, testing SAE engine no. 6 ...

station 281, testing SAE engine no. 10 ...

station 281, testing SAE engine no. 3 ...

station 281, testing SAE engine no. 7 ...

station 281, testing SAE engine no. 11 ...

station 281, testing SAE engine no. 0 ...

station 281, testing SAE engine no. 4 ...

station 281, testing SAE engine no. 8 ...

station 281, testing SAE engine no. 1 ...

station 281, testing SAE engine no. 5 ...

station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...

AES-CBC Known Answer Test:

Passed


```
station 281, testing SAE engine no. 10 ...  
station 281, testing SAE engine no. 3 ...  
station 281, testing SAE engine no. 7 ...  
station 281, testing SAE engine no. 11 ...  
station 281, testing SAE engine no. 0 ...  
station 281, testing SAE engine no. 4 ...  
station 281, testing SAE engine no. 8 ...  
station 281, testing SAE engine no. 1 ...  
station 281, testing SAE engine no. 5 ...  
station 281, testing SAE engine no. 9 ...  
station 281, testing SAE  
ms40 (ttyd0)
```

10

CHAPTER

Operational Commands

`request system zeroize` | **141**

`request vmhost zeroize no-forwarding` | **143**

request system zeroize

Syntax

```
request system zeroize
```

Release Information

Command introduced before Junos OS Release 9.0.

Command introduced in Junos OS Release 12.2 for MX Series routers.

Description

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to all Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as **root** and start the Junos OS CLI by typing **cli** at the prompt.

Required Privilege Level

maintenance

List of Sample Output

[request system zeroize on page 141](#)

Sample Output

request system zeroize

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

```
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

warning: zeroizing re0
Jul 27 22:25:53 jlaunchd: gkd-re (PID 5264) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: inet-process (PID 5267) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: periodic-packet-services (PID 5271) terminate signal 15
```

```

sent
Jul 27 22:25:53 jlaunchd: disk-monitoring (PID 5273) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: neighbor-liveness (PID 5307) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: event-processing (PID 5209) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: clksyncd-service (PID 5316) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ethernet-link-fault-management (PID 5321) terminate
signal 15 sent
Jul 27 22:25:53 jlaunchd: subscriber-management (PID 5323) terminate signal 15
sent
Jul 27 22:25:53 jlaunchd: shm-rtssdbd (PID 5325) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gstatd (PID 5326) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: rpcbind-service (PID 5330) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: icmd (PID 5332) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: pmcd (PID 5333) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ftp-inet-process (PID 5334) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: process-monitor (PID 5338) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: smg-service-telemetry (PID 5340) terminate signal 15
sent
Jul 27 22:25:53 jlaunchd: application-identification (PID 5341) terminate signal
15 sent
Jul 27 22:25:53 jlaunchd: resource-management (PID 5342) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: charged (PID 5346) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: license-service (PID 5351) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ntp (PID 6120) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gkd-chassis (PID 6121) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gkd-lchassis
.....

```

request vmhost zeroize no-forwarding

Syntax

```
request vmhost zeroize no-forwarding
```

Release Information

Command introduced in Junos OS Release 15.1F3 for the MX240, MX480, and MX960 routers.

Command introduced in Junos OS Release 15.1F5 for the MX2010 and MX2020 routers.

Description

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to both Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory-default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as the root user and start the Junos OS CLI by typing **cli** at the prompt.

Required Privilege Level

maintenance

List of Sample Output

[request vmhost zeroize no-forwarding on page 143](#)

Sample Output

request vmhost zeroize no-forwarding

```
user@host> request vmhost zeroize no-forwarding
```

```
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes

re0:
-----
warning: Vmhost will reboot and may not boot without configuration
```

```

warning: Proceeding with vmhost zeroize
Zeroize secondary internal disk ...
Proceeding with zeroize on secondary disk
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of secondary disk completed
Zeroize primary internal disk ...
Proceeding with zeroize on primary disk
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_rsa_key.pub
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_dsa_key
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of primary disk completed
Zeroize done
---(more)---
Waiting for PIDS: 6135.
.
Feb 16 14:59:33 jlaunchd: periodic-packet-services (PID 6181) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: smg-service (PID 6234) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: application-identification (PID 6236) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: ifstate-tracing-process (PID 6241) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: resource-management (PID 6243) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: charged (PID 6246) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: license-service (PID 6255) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: ntp (PID 6620) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: gkd-chassis (PID 6621) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: gkd-lchassis (PID 6622) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: routing (PID 6625) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: sonet-aps (PID 6626) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: remote-operations (PID 6627) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: class-of-service
.....

```