

Junos[®] OS

Common Criteria Configuration Guide for MX104 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 Configuration Guide for MX104 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 | vi

Documentation and Release Notes | vi

Documentation Conventions | vi

Documentation Feedback | ix

Requesting Technical Support | ix

Self-Help Online Tools and Resources | x

Creating a Service Request with JTAC | x

1

Common Criteria

Overview | 12

Understanding the Common Criteria Evaluated Configuration | 12

Understanding Common Criteria | 12

Supported Platforms and Hardwares | 13

Identifying Secure Product Delivery | 13

Understanding Management Interfaces | 14

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms | 15

Terminology | 15

Supported Cryptographic Algorithms | 16

Configuring Roles and Authentication Methods | 18

Understanding Roles and Services for Junos OS in FIPS Mode | 19

Security Administrator Role and Responsibilities | 19

FIPS User Role and Responsibilities | 20

What Is Expected of All FIPS Users | 20

Understanding the Operational Environment for Junos OS in FIPS Mode | 21

Hardware Environment for Junos OS in FIPS Mode | 21

Software Environment for Junos OS in FIPS Mode | 21

Critical Security Parameters | 22

Understanding Password Specifications and Guidelines for Junos OS | 25

Downloading Software Packages from Juniper Networks | 26

Installing Software on a Device | 26

Understanding Zeroization to Clear System Data | 28

Why Zeroize? | 29

When to Zeroize? | 29

Zeroizing the System | 30

Enabling FIPS Mode | 31

Configuring Security Administrator and FIPS User Identification and Access | 33

Configuring Security Administrator Access | 33

Configuring FIPS User Login Access | 35

Configuring Administrative Credentials and Privileges | 37

Understanding the Associated Password Rules for an Authorized Administrator | 37

Configuring a Network Device Collaborative Protection Profile Authorized Administrator | 39

Customize Time | 41

Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle Session | 41

Configuring Session Termination | 41

Sample Output for Local Administrative Session Termination | 43

Sample Output for Remote Administrative Session Termination | 43

Sample Output for User Initiated Termination | 44

Configuring SSH and Console Connection | 44

Configuring a System Login Message and Announcement | 44

Configuring SSH on the Evaluated Configuration | 45

Limiting the Number of User Login Attempts for SSH Sessions | 47

Sample Syslog Server Configuration on a Linux System | 48

Configuring Audit Log Options | 56

Configuring Audit Log Options in the Evaluated Configuration | 57

Configuring Audit Log Options for MX104 Devices | 57

Sample Code Audits of Configuration Changes | 58

Configuring Event Logging | 77

- Event Logging Overview | 77
- Configuring Event Logging to a Local File | 78
- Interpreting Event Messages | 78
- Logging Changes to Secret Data | 79
- Login and Logout Events Using SSH | 80
- Logging of Audit Startup | 81

Overview of VPNEP | 82

- VPNEP Configurations | 82
 - Configuring IPsec VPN Extended Package (EP) | 82
- IPsec VPN Configuration with Reference Identifier | 88
 - Sample IPsec VPN Configuration with IPv4 Address as Reference Identifier | 89
 - Sample IPsec VPN Configuration with FQDN as Reference Identifier | 96
 - Sample Configuration for Distinguished Name as Reference Identifier | 103
- Generating Certificate Signing Request (CSR) | 114
- Configuring Firewall Rules | 115

Performing Self-Tests on a Device | 121

- Understanding FIPS Self-Tests | 121

Operational Commands

- `request system zeroize` | 129

About the Documentation

IN THIS SECTION

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

Use this guide to configure and evaluate MX104 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 vii 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 vii 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

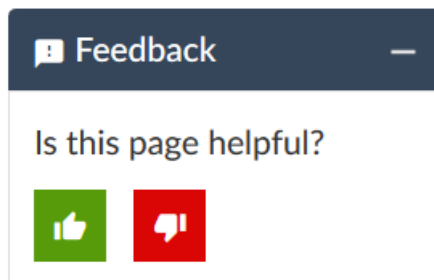
Table 2: Text and Syntax Conventions (*continued*)

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

Common Criteria

Overview | **12**

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms | **15**

Configuring Roles and Authentication Methods | **18**

Configuring Administrative Credentials and Privileges | **37**

Configuring SSH and Console Connection | **44**

Sample Syslog Server Configuration on a Linux System | **48**

Configuring Audit Log Options | **56**

Configuring Event Logging | **77**

Overview of VPNEP | **82**

Performing Self-Tests on a Device | **121**

Overview

IN THIS SECTION

- Understanding the Common Criteria Evaluated Configuration | 12
- Identifying Secure Product Delivery | 13
- Understanding Management Interfaces | 14

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/_CPP_ND_V2.1.pdf
- VPNEP—<https://www.niap-ccevs.org/Profile/Info.cfm?id=382>

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

NOTE: Junos OS Release 19.1R2 is certified for Common Criteria with FIPS mode enabled on MX104 device. For regulatory compliance information about Common Criteria, and FIPS for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#)

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

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 <https://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 <https://www.commoncriteriaportal.org/>.

Supported Platforms and Hardware

MX104 device in FIPS mode with the following hardware components are used to qualify NDcPPv2 certification with VPN-EP:

- Routing Engine: RE-MX-104 (https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/mx104-host-subsystem.html#id-mx104-routing-engine-overview)
- Crypto line card: MS-MIC-16G (https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/general/mic-mx-series-ms.html)

SEE ALSO

| [Identifying Secure Product Delivery](#) | 13

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.

Understanding Management Interfaces

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

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

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- Terminology | 15
- Supported Cryptographic Algorithms | 16

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*.

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. MX104 devices are certified at FIPS 140-2 Level 1.

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

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

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

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 [“Performing Self-Tests on a Device” on page 121](#).

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
IKEv1/v2	<ul style="list-style-type: none"> • Group14(modp2048) • Group 19 (P-256) • Group 20 (P-384) 	<ul style="list-style-type: none"> • RSA 2048 • RSA 4096 • Pre-SharedKey • ECDSAP-256 • ECDSAP-384 	<ul style="list-style-type: none"> • AES CBC 128 • AES CBC 192 • AES CBC 256 	<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256-128 • HMAC-SHA-384-192
IPsec ESP	IKEv1/v2with optional: <ul style="list-style-type: none"> • Group14(modp2048) • Group 19 (P-256) • Group 20 (P-384) 	<ul style="list-style-type: none"> • IKEv1/v2 	<ul style="list-style-type: none"> • AES CBC 128 • AES CBC 192 • AES CBC 256 • AES 128 GCM • AES 192 GCM • AES 256 GCM 	<ul style="list-style-type: none"> • HMAC-SHA-256-128
SSHv2	<ul style="list-style-type: none"> • dh-group14-sha1 • ECDH-sha2-nistp256 • ECDH-sha2-nistp384 • ECDH-sha2-nistp521 	Host (module): <ul style="list-style-type: none"> • ECDSA P-256 • SSH-RSA Client (user): <ul style="list-style-type: none"> • ECDSA P-256 • ECDSA P-384 • ECDSA P-521 • SSH-RSA 	<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

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

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

| [Performing Self-Tests on a Device](#) | 121

Configuring Roles and Authentication Methods

IN THIS SECTION

- [Understanding Roles and Services for Junos OS in FIPS Mode](#) | 19
- [Understanding the Operational Environment for Junos OS in FIPS Mode](#) | 21
- [Understanding Password Specifications and Guidelines for Junos OS](#) | 25
- [Downloading Software Packages from Juniper Networks](#) | 26
- [Installing Software on a Device](#) | 26
- [Understanding Zeroization to Clear System Data](#) | 28
- [Zeroizing the System](#) | 30
- [Enabling FIPS Mode](#) | 31
- [Configuring Security Administrator and FIPS User Identification and Access](#) | 33

Understanding Roles and Services for Junos OS in FIPS Mode

IN THIS SECTION

- [Security Administrator Role and Responsibilities | 19](#)
- [FIPS User Role and Responsibilities | 20](#)
- [What Is Expected of All FIPS Users | 20](#)

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 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.

Security Administrator performs all FIPS-mode-related configuration tasks and issue all statements and commands 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.

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 with FIPS-approved algorithms.
- 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.

SEE ALSO

| [Zeroizing the System](#) | 30

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

- [Hardware Environment for Junos OS in FIPS Mode](#) | 21
- [Software Environment for Junos OS in FIPS Mode](#) | 21
- [Critical Security Parameters](#) | 22

A Juniper Networks device 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 device in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the device that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the device that requires a cryptographic boundary for FIPS 140-2 compliance is a separate cryptographic module. There are two types of hardware with cryptographic boundaries in Junos OS in FIPS mode: one for each Routing Engine and one for entire chassis which includes encryption services PIC (MS-MIC).

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

FIPS mode on MX104 device is available in Junos OS Release 19.1R2 and later. The Junos OS in FIPS mode software environment is established after the Security Administrator successfully enables FIPS mode

on a device. 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 device.

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). The default password format in FIPS mode is SHA512. 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 device 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 device or Routing Engine as a cryptographic module.

Table 4 on page 23 lists CSPs on devices running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroize	Use
SSHv2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSHv2 session keys	Session key used with SSHv2 and as a Diffie-Hellman private key. Encryption: AES-128, AES-256. MACs: HMAC-SHA-1, HMAC-SHA-2-256, HMAC-SHA2-512. Key exchange: dh-group14-sha1, ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	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.

Table 4: Critical Security Parameters (*continued*)

CSP	Description	Zeroize	Use
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.

Local passwords are encrypted 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.

SEE ALSO

[Understanding Password Specifications and Guidelines for Junos OS | 25](#)

[Understanding Zeroization to Clear System Data | 28](#)

Understanding Password Specifications and Guidelines for Junos OS

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.

Downloading Software Packages from Juniper Networks

For MX104 router, download the following packages from the Juniper Networks website:

- jinstall-ppc-19.1R2.8-signed.tgz
- fips-mode-powerpc-19.1R2.8-signed.tgz
- jpfe-fips-powerpc-19.1R2.8-signed.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](#)

SEE ALSO

| [Installation and Upgrade Guide](#)

Installing Software on a Device

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

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

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks” on page 26](#).
2. If you have not already done so, connect to the console port on the device 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 device.

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 Junos OS image on the device:

```
user@device> request system software add <package> dualroot
```

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 device, 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, **jinstall-ppc-19.1R2.8-signed.tgz**.
 - **ftp://hostname/pathname/package.tgz**
 - **http://hostname/pathname/package.tgz**

6. Reboot the device to load the installation:

```
user@device> request system reboot
```

7. Once the router comes up with 19.1R2 build, copy and install **fips-mode** and **jpfe-fips** packages using **request system software add fips-mode-powerpc-19.1R2.8-signed.tgz** and **request system software add jpfe-fips-powerpc-19.1R2.8-signed.tgz** commands. Verify that the packages are successfully installed using **show version** command.

```
user@device:> show version
Hostname: hostname
Model: mx104
Junos: 19.1R2.8
JUNOS Base OS boot [19.1R2.8]
JUNOS Base OS Software Suite [19.1R2.8]
JUNOS Crypto Software Suite [19.1R2.8]
JUNOS Packet Forwarding Engine Support (TRIO) [19.1R2.8]
JUNOS Web Management [19.1R2.8]
JUNOS Online Documentation [19.1R2.8]
JUNOS SDN Software Suite [19.1R2.8]
JUNOS Services Application Level Gateways [19.1R2.8]
JUNOS Services COS [19.1R2.8]
JUNOS Services Jflow Container package [19.1R2.8]
JUNOS Services Stateful Firewall [19.1R2.8]
JUNOS Services NAT [19.1R2.8]
JUNOS Services RPM [19.1R2.8]
JUNOS Services Captive Portal and Content Delivery Container package [19.1R2.8]
JUNOS Macsec Software Suite [19.1R2.8]
JUNOS Services Crypto [19.1R2.8]
JUNOS Services IPSec [19.1R2.8]
JUNOS DP Crypto Software Suite [19.1R2.8]
JUNOS py-base-powerpc [19.1R2.8]
JUNOS py-extensions-powerpc [19.1R2.8]
JUNOS jsd [powerpc-19.1R2.8-jet-1]
JUNOS Kernel Software Suite [19.1R2.8]
JUNOS Routing Software Suite [19.1R2.8]
JUNOS FIPS mode utilities [19.1R2.8]
JUNOS Packet Forwarding Engine FIPS Support [19.1R2.8]
```

Understanding Zeroization to Clear System Data

IN THIS SECTION

- [Why Zeroize? | 29](#)
- [When to Zeroize? | 29](#)

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.

The Security Administrator initiates the zeroization process by entering the **request system zeroize** operational command for MX104 devices from the CLI after enabling FIPS mode. Use of this command is restricted to the Security Administrator. (To zeroize the system *before* enabling FIPS mode, use the **request system zeroize** command to completely wipe-out older CSPs and scrub memory.)

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

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

When to Zeroize?

As Security Administrator, perform zeroization in the following situations:

- **Before enabling FIPS mode of operation:** To prepare your device 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 device for non-FIPS operation, perform zeroization before disabling FIPS mode on the device.

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.

SEE ALSO

[Zeroizing the System](#) | 30

Zeroizing the System

As Security Administrator, you run the **request system zeroize** command to remove all user-created files from a device and replace the user data with zeros. This command completely erases all configuration information on the Routing Engines, including all rollback configuration files and plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, and IPsec.

NOTE: Zeroization is required on MX104 device before you upgrade in FIPS mode.

To zeroize your device:

1. From the CLI, enter

```
security-administrator@device> 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:
```

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.

SEE ALSO

Enabling FIPS Mode

As Security Administrator, you must establish a root password conforming to the FIPS password requirements in [“Understanding Password Specifications and Guidelines for Junos OS” on page 25](#). When you enable FIPS mode in Junos OS on the device, 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” on page 28](#) section for details.
2. After the device comes up in 'Amnesiac mode', login using username **root** and password "" (blank).

```
Amnesiac (ttyu0)
login: root
--- JUNOS 19.1R2.8 built 2018-06-28 03:01:33 UTCC
% cli
root> edit
Entering configuration mode
```

3. Configure root authentication with at least 10 characters or more.

```
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. Configure security-administrator and login using security-administrator credentials.

5. Install **fips-mode** package needed for Routing Engine Known Answer Tests (KATS).

```
security-administrator@host> request system software add /var/tmp/fips-mode-powerpc-19.1R2.8-signed.tgz
no-validate
Installing package '/var/tmp/fips-mode-powerpc-19.1R2.8-signed.tgz' ...
Verified fips-mode-powerpc-19.1R2.8 signed by PackageProductionEc_2018 method
ECDSA256+SHA256
Mounted fips-mode-powerpc package on /dev/md15...
Verified manifest signed by PackageProductionEc_2018 method ECDSA256+SHA256
Verified fips-mode-powerpc-19.1R2.8 signed by PackageProductionEc_2018 method
ECDSA256+SHA256
Saving package file in /var/sw/pkg/fips-mode-powerpc-19.1R2.8-signed.tgz ...
Saving state for rollback ...
```

6. Install **jpfe-fips** package needed for MS-MIC Known Answer Tests (KATS).

```
security-administrator@host> request system software add /var/tmp/jpfe-fips-powerpc-19.1R2.8-signed.tgz
no-validate
Installing package '/var/tmp/jpfe-fips-powerpc-19.1R2.8-signed.tgz' ...
Verified jpfe-fips-powerpc-19.1R2.8.tgz signed by PackageProductionEc_2018 method
ECDSA256+SHA256
Adding jpfe-fips-powerpc...
Mounted jpfe-fips package on /dev/md16...
Verified manifest signed by PackageProductionEc_2018 method ECDSA256+SHA256
Verified jpfe-fips-powerpc-19.1R2.8 signed by PackageProductionEc_2018 method
ECDSA256+SHA256
Saving package file in /var/sw/pkg/jpfe-fips-powerpc-19.1R2.8-signed.tgz ...
Saving state for rollback ...
```

7. 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]
security-administrator@host# 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
[edit]
security-administrator@host# run request system reboot

```

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

```
security-administrator@host:fips>
```

SEE ALSO

[Understanding Password Specifications and Guidelines for Junos OS | 25](#)

Configuring Security Administrator and FIPS User Identification and Access

IN THIS SECTION

- [Configuring Security Administrator Access | 33](#)
- [Configuring FIPS User Login Access | 35](#)

Security Administrators 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 device with the root password if you have not already done so, and enter configuration mode:

```
root@hostname# edit
  Entering configuration mode
[edit]
root@hostname#
```

2. Name the user **security-administrator** 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@hostname# set system login user username uid value class class-name
```

For example:

```
[edit]
root@hostname# set system login user security-administrator uid 6400 class super-user
```

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS](#)” on [page 25](#), 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@hostname# set system login user username class class-name authentication (plain-text-password |
  encrypted-password)
```

For example:

```
[edit]
root@hostname# set system login user security-administrator class super-user authentication
  plain-text-password
```

4. Optionally, display the configuration:

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

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

```
[edit]
root@hostname# commit
commit complete
root@hostname# exit
```

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 device with your Security Administrator password if you have not already done so, and enter configuration mode:

```
security-administrator@hostname:fips> edit
  Entering configuration mode
[edit]
security-administrator@hostname: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**, **network**, **resetview**, and **view-configuration**.

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

```
[edit]
security-administrator@hostname:fips# set system login user username uid value class class-name
```

For example:

```
[edit]
security-administrator@hostname:fips# set system login user fips-user1 uid 6401 class read-only
```

- Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS](#)” on [page 25](#), 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]
security-administrator@hostname:fips# set system login user username class class-name authentication
    (plain-text-password | encrypted-password)
```

For example:

```
[edit]
security-administrator@hostname:fips# set system login user fips-user1 class read-only authentication
    plain-text-password
```

- Optionally, display the configuration:

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

- If you are finished configuring the device, commit the configuration and exit:

```
[edit]  
security-administrator@hostname:fips# commit  
security-administrator@hostname:fips# exit
```

Configuring Administrative Credentials and Privileges

IN THIS SECTION

- [Understanding the Associated Password Rules for an Authorized Administrator | 37](#)
- [Configuring a Network Device Collaborative Protection Profile Authorized Administrator | 39](#)
- [Customize Time | 41](#)
- [Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle Session | 41](#)

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: Do 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]

```
security-administrator@host:fips# 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]

```
security-administrator@host:fips# 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 3.

[edit]

```
security-administrator@host:fips# set system login password minimum-changes 3
```

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

[edit]

```
security-administrator@host:fips# set system login password format sha512
```

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.

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 NDcPPv2.1 authorized administrator must have all permissions, including the ability to change the device configuration.

To configure an authorized administrator:

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

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

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

```
[edit]
security-administrator@host:fips# set system login password format sha512
```

3. Commit the changes.

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

4. Define your NDcPPv2.1 user authorized administrator.

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

or

```
[edit]
```

```
security-administrator@host:fips# set system login user NDcPPv2-user class security-admin authentication
plain-text-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]
security-administrator@host:fips# 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]
security-administrator@host:fips# set system services ssh log-key-changes
```

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.

7. Commit the changes.

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

Customize Time

To customize time, disable NTP and set date.

- Disable NTP.

```
[edit]
user@host# deactivate groups global system ntp
user@host# deactivate system ntp
user@host# commit
user@host# exit
```

- Set date and time. Date and time format is YYYYMMDDHHMM.ss

```
[edit]
user@host# set date 201803202034.00
user@host# set cli timestamp
```

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

IN THIS SECTION

- [Configuring Session Termination | 41](#)
- [Sample Output for Local Administrative Session Termination | 43](#)
- [Sample Output for Remote Administrative Session Termination | 43](#)
- [Sample Output for User Initiated Termination | 44](#)

Configuring Session Termination

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

1. Set the idle timeout.

```
[edit]
```

```
security-administrator@host:fips# set system login class security-admin idle-timeout 2
```

2. Configure the login access privileges.

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

3. Commit the configuration.

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

```
commit complete
```

4. Set the password.

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

5. Define login class.

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

6. Commit the configuration.

```
[edit]
security-administrator@host:fips# 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 19.1R2.8 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 19.1R2.8 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 19.1R2.8 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 19.1R2.8 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NdcPPv2-user@host> exit

Connection to host closed.
```

Configuring SSH and Console Connection

IN THIS SECTION

- [Configuring a System Login Message and Announcement | 44](#)
- [Configuring SSH on the Evaluated Configuration | 45](#)
- [Limiting the Number of User Login Attempts for SSH Sessions | 47](#)

Configuring a System Login Message and Announcement

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

To configure a system login message through console or management interface, use the following command:

```
[edit]
security-administrator@host:fps# set system login message login-message-banner-text
```

To configure system announcement, use the following command:

```
[edit]
security-administrator@host:fps# 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

SSH through remote management interface is allowed in the evaluated configuration. If the existing SSH connection is broken unintentionally, for example due to 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 need 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]
security-administrator@host:fips# set system services ssh hostkey-algorithm ssh-ecdsa
security-administrator@host:fips# set system services ssh hostkey-algorithm no-ssh-dss
security-administrator@host:fips# set system services ssh hostkey-algorithm ssh-rsa
```

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

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

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

```
[edit]
security-administrator@host:fips# set system services ssh macs hmac-sha1
security-administrator@host:fips# set system services ssh macs hmac-sha2-256
security-administrator@host:fips# set system services ssh macs hmac-sha2-512
```

4. Specify the ciphers allowed for protocol version 2.

```
[edit]
security-administrator@host:fips# set system services ssh ciphers aes128-cbc
security-administrator@host:fips# set system services ssh ciphers aes256-cbc
security-administrator@host:fips# set system services ssh ciphers aes128-ctr
security-administrator@host:fips# 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]
security-administrator@host:fips# 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]
security-administrator@host:fips# 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]
security-administrator@host:fips# 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]
security-administrator@host:fips# 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]
security-administrator@host:fips# 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.

Sample 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 device. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.

Use the configuration details and establish a session between the target of evaluation (TOE) and the audit server u. Examine the traffic that passes between the audit server and the TOE during several activities, and the generated audit data to be transferred to the audit server.

Examine the TOE Summary Specification (TSS) to ensure that it specifies the means by which the audit data is transferred to the external audit server and how the trusted channel is provided.

The NDcPP logs capture the following events:

- Committed changes
- System startup

- Login and logout of users
- Failure to establish an SSH session
- Establishment or termination of an SSH session
- Changes to the system time
- Initiation of a system update

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 pass phrase. The storage locations for the **syslog-monitor** key pair is displayed.

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

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

4. Set up NETCONF with SSH.

```
[edit system services]
security-administrator@host:fips# set netconf ssh
```

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

```
[edit system services]
security-administrator@host:fips# set syslog file messages any any
commit
```

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

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

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.

```
security-administrator@host:fips# $ssh syslog-mon@NDcPP_TOE -s netconf > test.out
```

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

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

10. The examples for syslog messages are listed below. Monitor the event log generated for admin actions on TOE are received on 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 logging and remote event logged in syslog server and record the particular software (name, version) 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 ]-----+
```



```

<capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>

    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>

<capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</capability>

    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
</capabilities>
<session-id4129/session-id>
</hello>
]]>]]>

```

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

```

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

```

Net configuration channel

```
host@nms5-vm-linux2 ~]$ ssh syslog-mon@starfire -s netconf
```

```
this is NDCPP test device
```

```

<!-- No zombies were killed during the creation of this user interface --
<!-- user syslog-mon, class j-monitor -><hello>

```

```

<capabilities>
  <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
  <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>

<capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>

  <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>

<capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</capability>

  <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
  <capability>http://xml.juniper.net/dmi/system/1.0</capability>
</capabilities>
<session-id4129/session-id>
</hello>
]]>]]>

```

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

```

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
```

```
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

```

Configuring Audit Log Options

IN THIS SECTION

- [Configuring Audit Log Options in the Evaluated Configuration | 57](#)
- [Sample Code Audits of Configuration Changes | 58](#)

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

- [Configuring Audit Log Options for MX104 Devices | 57](#)

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

Configuring Audit Log Options for MX104 Devices

To configure audit log options for MX104 devices:

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

```
[edit system syslog]
security-administrator@host:fips# set archive files 2
```

2. Specify the file in which to log data.

```
[edit system syslog]
security-administrator@host:fips# set file syslog any any
```

3. Specify the size of files to be archived.

```
[edit system syslog]
security-administrator@host:fips# set file syslog archive size 10000000
```

4. Specify the priority and facility in messages for the system logging facility.

```
[edit system syslog]
security-administrator@host:fips# set file syslog explicit-priority
```

5. Log system messages in a structured format.

```
[edit system syslog]
security-administrator@host:fips# set file syslog structured-data
```

SEE ALSO

| [Sample Code Audits of Configuration Changes](#) | 58

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.

```

security-administrator@host:fips# 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 60 shows sample for syslog auditing for NDcPPv2.1:

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	
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	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
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],</p>

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			ssh-connection '10.1.5.153 36784 10.1.2.68 22', client-mode 'cli' Unsuccessful Remote Login 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</p>

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			<p>10.1.2.68 22', client-mode 'cli'</p> <p>Unsuccessful Remote Login</p> <p>Jan 3 09:26:56 sshd: SSHD_LOGIN_FAILED: Login failed for user 'test1' from host '10.1.5.153'</p>
FIA_UAU.7	None	None	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	<p>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'</p>
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	

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
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'
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

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FTA_SSL.4	The termination of an interactive session.	None	<p>Local</p> <p>Jan 3 11:47:25 mgd[52521]: UI_LOGOUT_EVENT: User 'root' logout</p> <p>Remote</p> <p>Jan 3 11:43:33 sshd[52425]: Received disconnect from 10.1.5.153 port 36800:11: disconnected by user</p>
FTA_TAB.1	None	None	
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'

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted or received during session establishment	

Table 5: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			<p>Nov 9 20:24:13 ikev2_allocate_exchange_data: Successfully allocated exchange data for SA 88fbc00 Nov 9 20:24:13 ikev2_allocate_exchange_data_info: Successfully allocated Info exchange data for SA 88fbc00 ED 88ab028 Nov 9 20:24:13 ikev2_allocate_exchange_data: Successfully allocated exchange data for SA 88fb300 Nov 9 20:24:13 ikev2_allocate_exchange_data_info: Successfully allocated Info exchange data for SA 88fb300 ED 8927028 Nov 9 20:24:13 [20.1.1.1 <-> 30.1.1.2] ikev2_decode_encr: [8920400/88fbc00] Packet decrypted successfully Nov 9 20:24:13 [20.1.1.1 <-> 30.1.1.2] ikev2_delete_notify_done_data: Received success IKE SA 88fbc00 delete notification Nov 9 20:24:13 [20.1.1.1 <-> 30.1.1.2] ikev2_free_exchange_data_info: Successfully freed Info exchange data from SA 88fbc00 Nov 9 20:24:13 [20.1.1.1 <-> 30.1.1.2] ikev2_free_exchange_data: Successfully freed exchange data from SA 88fbc00 Nov 9 20:24:13</p>

Table 5: Auditable Events (continued)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			[20.1.1.1 <-> 30.1.1.2] ikev2_decode_encr: [8921080/88fb300] Packet decrypted successfully
FIA_X509_EXT.1	Session establishment with CA	Entire packet contents of packets transmitted or received during session establishment	Nov 9 20:24:14 [20.1.1.1 <-> 30.1.1.2] ikev2_decode_auth: [8920e00/88fbc00] AUTH(method = RSA Sig (1), len = 256, data = 7a3da09a 068ac628 5e0abaf9 dcc41c33 7bdf7073 f654835a aef2e5bf f71288fc 207bed57 8b5ce79a 1112be79 a8616396 5984a7f1 834ba83d 0fe75219 8d10eeb7 2e730445 0c610fe1 e75aa728 04 Nov 9 20:24:21 ikev2_decode_auth: [8921300/88fb300] AUTH(method = RSA Sig (1), len = 256, data = 9ecf8df6 fb44582a 5e1acbcc bc38d392 d255fabb d3859e39 3ac6b82d 8f5f2dd3 d4943772 f0874829 f7a6c0bf dc0bc85b 6f0a86e5 864b8500 20108fca 249adfbcb1355265 489e0b32 346aeac2 a5

Table 5: Auditable Events (*continued*)

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	Time of Log: 2017-11-09 21:02:03 PST, Filter: pfe, Filter action: accept, Name of interface: ms-4/0/0.1 Name of protocol: TCP, Packet Length: 52, Source address: 40.1.1.2:10799, Destination address: 10.1.1.1:22
FPF_RUL_EXT.1	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets	Jan 8 01:08:09 bm-b (FPC Slot 2, PIC Slot 0) ms40 mspmand[249]: CPU zone change GREEN=>RED (98.98 %) Jan 8 01:08:09 bm-b (FPC Slot 2, PIC Slot 0) ms40 mspmand[249]: CPU utilization (98.98 percent) exceeded threshold, packets may be dropped Jan 8 01:08:09 bm-b (FPC Slot 2, PIC Slot 0) ms40 mspmand[249]: CPU trap sent successfully

SEE ALSO

[Configuring Audit Log Options in the Evaluated Configuration](#) | 57

Configuring Event Logging

IN THIS SECTION

- [Event Logging Overview | 77](#)
- [Configuring Event Logging to a Local File | 78](#)
- [Interpreting Event Messages | 78](#)
- [Logging Changes to Secret Data | 79](#)
- [Login and Logout Events Using SSH | 80](#)
- [Logging of Audit Startup | 81](#)

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.

SEE ALSO

| [Interpreting Event Messages](#) | 78

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;
}
```

SEE ALSO

| [Event Logging Overview](#) | 77

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 79](#) 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	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> • MMM-DD HH:MM:SS.MS+/-HH:MM, is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). • YYYY-MM-DDTHH:MM:SS.MSZ is the year, month, day, hour, minute, second and millisecond in UTC. 	Feb 27 02:33:04 is the timestamp expressed as local time in the United States. 2012-02-27T09:17:15.719Z is 2:33 AM UTC on 27 Feb 2012.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	4153
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
username	Username of the user initiating the event.	"admin"
message-text	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

SEE ALSO

[Event Logging Overview](#) | [77](#)

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]
```

SEE ALSO

[Interpreting Event Messages](#) | 78

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
```


SEE ALSO

| [Interpreting Event Messages](#) | 78

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:

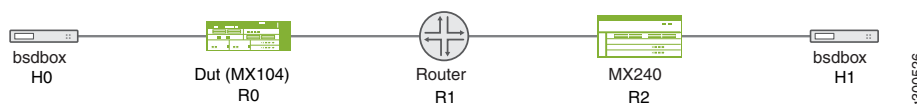
```
Dec 20 23:17:35 bilbo syslogd: exiting on signal 14
Dec 20 23:17:35 bilbo syslogd: restart
Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128)
    exited with status=1
Dec 20 23:17:42 bilbo /kernel:
Dec 20 23:17:53 init: syslogd (PID 19200) started
```

SEE ALSO

| [Login and Logout Events Using SSH](#) | 80

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



VPNEP Configurations

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	Maturred	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: juniperaA
Subject string:
  C=US, ST=MD, CN=juniperaA
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

```

```

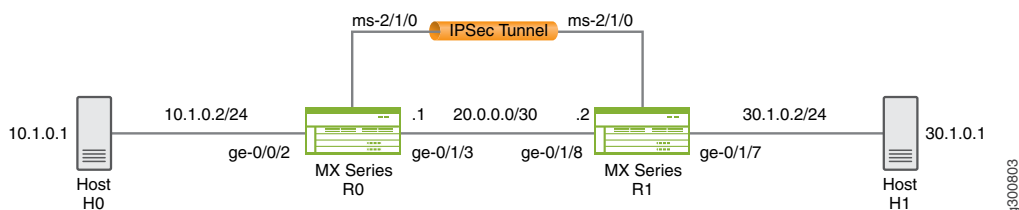
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBAjCBpwIBADATMREwDwYDVQQDEwgxMS4wLjEuMjBZMBMGBYqGSM49AgEGCCqG
SM49AwEHA0IABLRebeXGFF+AnH6I0AQu8gFQwOCbAm89wazpUpQs5RIGiVfYGgV1
xrwTGcQoKYc+a8PqJ7EQcffSttdQ1fUG9KqgMjAwBgkqhkiG9w0BCQ4xIzAhMB8G
AlUdEQQYMBaBFCJiYWxhamlAanVuaXBldi5uZXQiMAwGCCqGSM49BAMCBQADSAAw
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-MIC 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

Performing Self-Tests on a Device

IN THIS SECTION

- [Understanding FIPS Self-Tests | 121](#)

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that a device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode 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 device performs the following series of known answer test (KAT) self-tests:

- **kernel_kats**—KAT for kernel cryptographic routines
- **md_kats**—KAT for libmd and libc
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **quicksec_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **xlp_kats**—KAT for Multiservices MIC cryptographic implementation

The KAT self-tests are performed automatically at startup and reboot. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and ECDSA key pairs, and manually entered keys.

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

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

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

For MX104 device:

```

    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-ECB 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:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   FIPS ECDSA Known Answer Test:                   Passed
mgd:   FIPS ECDH Known Answer Test:                   Passed
mgd:   FIPS RSA Known Answer Test:                     Passed
mgd:   DES3-CBC Known Answer Test:                   Passed
mgd:   HMAC-SHA1 Known Answer Test:                   Passed
mgd:   HMAC-SHA2-224 Known Answer Test:               Passed
mgd:   HMAC-SHA2-256 Known Answer Test:               Passed
mgd:   HMAC-SHA2-384 Known Answer Test:               Passed
mgd:   HMAC-SHA2-512 Known Answer Test:               Passed
mgd:   AES-CBC Known Answer Test:                     Passed
mgd:   AES-GCM Known Answer Test:                     Passed
mgd:   ECDSA-SIGN Known Answer Test:                  Passed
mgd:   KDF-IKE-V1 Known Answer Test:                  Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:              Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test: Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:         Passed
mgd: Testing QuickSec 7.0 KATS:

```

```

mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
  mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: SSH-ECDSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing QuickSec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing SSH IPsec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: Testing file integrity:
mgd: File integrity Known Answer Test: Passed
mgd: Testing crypto integrity:
mgd: Crypto integrity Known Answer Test: Passed
mgd: Expect an exec Authentication error...
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error

```

```
mgd: FIPS Self-tests Passed
mgd: commit complete
```

For MX104 router, below KATS will run on MS-MIC:

```
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:
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 ...
```

Passed

```

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.  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
ms00 (ttyd0)

```

2

CHAPTER

Operational Commands

[request system zeroize](#) | **129**

request system zeroize

Syntax

```
request system zeroize  
<media>  
<local>
```

Release Information

Command introduced before Junos OS Release 9.0.

Command introduced in Junos OS Release 11.2 for EX Series devices.

Option **media** added in Junos OS Release 11.4 for EX Series devices.

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

Option **local** added in Junos OS Release 14.1.

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.

To completely erase user-created data so that it is unrecoverable, use the **media** option in non FIPS mode.

Required Privilege Level

maintenance

List of Sample Output

[request system zeroize on page 129](#)

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
Terminated
Waiting (max 60 seconds) for system process `vnlru_mem' to
stop...root@nms5-mx104-done
Waiting (max 60 seconds) for system process `vnlru' to stop...c% Terminated
done
Waiting (max 60 seconds) for system process `bufdaemon' to stop...Jul  9 14:07:04
init: iccp-servidone
Waiting (max 60 seconds) for system process `syncer' to stop...ce (PID 3069) te
Syncing disks, vnodes remaining...2 rminate signal 15 sent

Jul  9 14:07:05 init: ddos-service (PID 3070) terminate signal 15 sent

Jul  9 14:07:05 init: nfsd-service (PID 3071) terminate signal 15 sent

Jul  9 14:07:05 init: mspd (PID 3072) terminate signal 15 sent

Jul  9 14:07:05 init: mountd-service (PID 3073) terminate signal 15 sent

Jul  9 14:07:05 init: subscriber-management-helper (PID 3075) terminate signal 15
sent

Jul  9 14:07:05 init: sflow-service (PID 3076) terminate signal 15 sent

Jul  9 14:07:05 init: dot1x-protocol (PID 3077) terminate signal 15 sent

Jul  9 14:07:05 init: commit-syncd (PID 3078) terminate signal 15 sent

Jul  9 14:07:05 init: jsd (PID 3079) terminate signal 15 sent

Jul  9 14:07:05 init: xmlproxyd (P4 ID 3080) terminate signal 15 sent

Jul  9 14:07:05 init: overlay-ping-traceroute (PID 3081) terminate signal 15 sent

Jul  9 14:07:05 init: alarm-management (PID 3084) terminate signal 15 sent

Jul  9 14:07:05 init: SDN-Telemetry (PID 3085) terminate signal 15 sent

Jul  9 14:07:05 init: stats-agent (PID 3086) terminate signal 15 sent

```

```

Jul  9 14:07:05 init: internal-routing-service (PID 3087) terminate signal 15 sent

Jul  9 14:07:05 init: firewall (PID 3088) terminate signal 15 sent

Jul  9 14:07:05 init: pfed (PID 3089) terminate signal 15 sent

3 2 0 0 0 done

syncing disks... All buffers synced.
Uptime: 17m28s
recorded reboot as normal shutdown
Rebooting...
... 9 ... 8 ... 7 ... 6 ... 5 ... 4 ... 3 ... 2 ... 1 ... 0

U-Boot 2011.12 (Aug 29 2013 - 15:55:06)
Build 600600

CPU0:  P5021, Version: 2.1, (0x82050021)
Core:  E5500, Version: 1.2, (0x80240012)
Clock Configuration:
      CPU0:1800 MHz, CPU1:1800 MHz,
      CCB:600  MHz,
      DDR:600  MHz (1200 MT/s data rate) (Asynchronous), LBC:37.500 MHz
      FMAN1: 450 MHz
      FMAN2: 300 MHz
L1:    D-cache 32 kB enabled
      I-cache 32 kB enabled
Press Ctrl-D to enter SLOWTEST mode
Bootcpld      : Ver 1 Rev 13 (Built 1-5-13)
U-boot expects : Ver 1 Rev 9 (Compatible)
Reboot Reason : 0x0100 (SW Initiated)
Boot Bank     : bank0
Board         : MX104 RE 2.4 (S/N CAKH3077)
I2C:  ready
DRAM:  Initializing....using SPD
Detected UDIMM XY1368E4GMPWP-JP
      4096 MB (3968 MB shall be used)
3.9 GiB (DDR3, 64-bit, CL=8, ECC on)
Quick testing memory 0x00000000 - 0xf7ffffff
Lines... regions...patterns... OK
POST memory PASSED
Flash: 4 MiB
L2:    512 KB enabled
Corenet Platform Cache: 1024 KB enabled

```

```

SERDES: bank 1 disabled
SERDES: bank 3 disabled
Using macaddr 64:c3:d6:b8:49:17 from EEPROM
USB HUB initializing ... OK
In:    serial
Out:   serial
Err:   serial
USB:   Register 10011 NbrPorts 1
USB EHCI 1.00
scanning bus for devices... 3 USB Device(s) found
      scanning bus for storage devices... 1 Storage Device(s) found
Net:   Initializing Fman
Fman1: Uploading microcode version 106.1.8
FM1@DTSEC4 [PRIME]
Bootlist = < USB0 USB1 NAND-FLASH0(as) >
Junos requested bootdev = USB0
Internal storage is dual-rooted.
Will attempt to boot from NAND-FLASH0-slice1 (active)
Press Ctrl-C to abort autoboot:  1___  0## Starting application at 0x00010080 ...
Consoles: U-Boot console

```

```

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.4

```

```

(rajatjain@svl-junos-pool53.juniper.net, Fri Jun  8 11:58:22 PDT 2012)

```

```

Memory: 3968MB

```

```

.....

```