Junos® OS for MX Series Routers, Release 14.1R4

FIPS

This guide is only for Junos OS MX Series routers, Junos OS Release 14.1R4. Any references to M, PTX, and T Series routers in this guide are not applicable.

Release
14.1R4

Modified: 2015-12-29
Revision 1

Copyright © 2016, Juniper Networks, Inc.

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

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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 for M, MX, PTX, and T Series Routers FIPS
Release 14.1R4
Copyright © 2016, 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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

About the Documentation

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

Supported Platforms

For the features described in this document, and to operate in accordance with the FIPS certification, Table 1 on page vii shows the platforms that are supported and their install images.

Table 1: Supported Platforms and Install Images

Platform	Install Image
M Series Multiservice Edge Routers	
M7i	jinstall-14.1R4.5-domestic-signed.tgz
M10i	jinstall-14.1R4.5-domestic-signed.tgz
M120	jinstall-14.1R4.5-domestic-signed.tgz
M320	jinstall-14.1R4.5-domestic-signed.tgz

Copyright © 2016, Juniper Networks, Inc.

Table 1: Supported Platforms and Install Images *(continued)*

Platform	Install Image
MX Series 3D Universal Edge Routers	
MX240	jinstall-14.1R4.5-domestic-signed.tgz
MX480	jinstall-14.1R4.5-domestic-signed.tgz
MX960	jinstall-14.1R4.5-domestic-signed.tgz
MX2010	jinstall64-14.1R4.5-domestic-signed.tgz
MX2020	jinstall64-14.1R4.5-domestic-signed.tgz
PTX Series Packet Transport Routers	
PTX3000	jinstall64-14.1R4.5-domestic-signed.tgz
PTX5000	jinstall64-14.1R4.5-domestic-signed.tgz
T Series Core Routers (Multichassis-Enabled IP/MPLS)	
T640	jinstall-14.1R4.5-domestic-signed.tgz
T1600	jinstall64-14.1R4.5-domestic-signed.tgz
T4000	jinstall64-14.1R4.5-domestic-signed.tgz

Documentation Conventions

Table 2 on page ix defines notice icons used in this guide.

Copyright © 2016, Juniper Networks, Inc.

Table 2: 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 3 on page ix defines the text and syntax conventions used in this guide.

Table 3: 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*

Copyright © 2016, Juniper Networks, Inc.

Table 3: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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 *metric*>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.

Copyright © 2016, Juniper Networks, Inc.

- 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 J-Care or JNASC 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

Copyright © 2016, Juniper Networks, Inc.

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

Copyright © 2016, Juniper Networks, Inc.

PART 1

Junos OS in FIPS Mode for M, MX, PTX, and T Series Routers

Copyright © 2016, Juniper Networks, Inc.

 Copyright © 2016, Juniper Networks, Inc.

CHAPTER 1

Junos OS in FIPS Mode Overview—Environment and Requirements

Understanding Junos OS in FIPS Mode

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, the Juniper Networks RE-1800 Routing Engine on Juniper Networks MX Series 3D Universal Edge, T Series Routers, M Series Multiservice Edge Routers, and PTX Series Packet Transport Routers running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

Copyright © 2016, Juniper Networks, Inc.

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

The *Crypto Officer* enables FIPS mode in Junos OS Release 14.1R4 and sets up keys and passwords for the system and other *FIPS users* who can view the configuration. Both user types can also perform normal configuration tasks on the router (such as modify interface types) as individual user configuration allows.

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

About the Cryptographic Boundary on Your Router

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

CAUTION: **Virtual Chassis features are not supported in FIPS mode—they have not been tested by Juniper Networks. Do not configure a Virtual Chassis in FIPS mode.**

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

How FIPS Mode Differs from Non-FIPS Mode

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

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and MD5 are disabled.

Copyright © 2016, Juniper Networks, Inc.

- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters long.

For specific configuration limitations and restrictions, see "Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode" on page 24.

How Junos OS in FIPS Mode Differs from Junos-FIPS

Junos OS in FIPS mode is an operating mode of Junos OS that you enable from the Junos OS command-line interface (CLI). In contrast, the *Junos-FIPS image* is a separately downloadable Junos OS image available for Juniper Networks MX Series routers and SRX Series Services Gateways.

Junos OS in FIPS mode is available only on the routers listed in Table 1 on page vii that are running Junos OS Release 14.1R4 and later.

Validated Version of Junos OS in FIPS Mode

Juniper Networks submits one Junos OS release per year—Junos OS Release 14.1R4, for example—to the National Institute of Standards and Technology (NIST) for validation. To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (http://www.juniper.net/) or the National Institute of Standards and Technology site at http://csrc.nist.gov/cryptval/140-1/1401val.htm.

How to Use FIPS Documentation

For configuration and operational tasks that are specific to FIPS mode on M Series, MX Series, PTX Series, and T Series routers, be sure to use the documentation for Junos OS in FIPS mode. Do not use the documentation for Junos in FIPS mode statements and commands because the syntax and options might not apply to FIPS mode.

Related Documentation

- Identifying Secure Delivery on page 5
- *Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode*
- Configuration Statements for Junos OS in FIPS Mode on page 53
- Operational Commands for Junos OS in FIPS Mode on page 69

Identifying Secure 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 an appliance 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.

Copyright © 2016, Juniper Networks, Inc.

- 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, 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 in to the Juniper Networks online customer support portal at https://www.juniper.net/customers/csc/management 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 FIPS Mode Terminology and Supported Cryptographic Algorithms

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

- FIPS Terminology on page 7
- Supported Cryptographic Algorithms on page 9

Copyright © 2016, Juniper Networks, Inc.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects. For details, see "Understanding the Operational Environment for Junos OS in FIPS Mode" on page 16

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. M Series, MX Series, PTX Series, and T Series routers are certified at FIPS 140-2 Level 1. For fixed-configuration routers, the cryptographic module is the router case. For modular routers, the cryptographic module is the Routing Engine.

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a router. For details, see "Understanding Roles and Services for Junos OS in FIPS Mode" on page 14.

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 Crypto Officer assumes to perform physical maintenance or logical maintenance services such as hardware or software diagnostics. For FIPS 140-2 compliance, the Crypto Officer 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.**

Hashing—A message authentication method that applies a cryptographic technique iteratively to a message of arbitrary length and produces a hash *message digest* or *signature* of fixed length that is appended to the messzage when sent.

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

Copyright © 2016, Juniper Networks, Inc.

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

NOTE: An IPsec security association (SA) is required for routers running Junos OS in FIPS mode for the following reasons:

- Because the cryptographic boundary on modular routers is the Routing Engine, M Series, MX Series, PTX Series, and T Series routers with redundant Routing Engines running Junos OS in FIPS mode require an internal, manual IPsec SA between the Routing Engines for secure communication.

For more information, see "Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode" on page 20.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "Understanding FIPS Self-Tests" on page 11.

SA—Security association (SA). A connection between hosts that allows them to communicate securely by defining, for example, how they exchange private keys. As Crypto Officer, you must manually configure an internal SA on routers running Junos OS in FIPS mode. All values, including the keys, must be statically specified in the configuration. On routers with more than one Routing Engine, the configuration must match on both ends of the connection between the Routing Engines. For communication to take place, each Routing Engine must have the same configured options, which need no negotiation and do not expire. For more information, see "Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode" on page 20.

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

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

Zeroization—Erasure of all CSPs and other user-created data on a router before its operation as a FIPS cryptographic module—or in preparation for repurposing the router for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command. For details, see "Understanding Zeroization to Clear System Data for FIPS Mode" on page 10.

Copyright © 2016, Juniper Networks, Inc.

Supported Cryptographic Algorithms

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

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

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

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

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

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

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

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

RSA—Algorithm for public key cryptography that is based on the presumed difficulty of factoring large integers of up to 2048 bits. The RSA algorithm involves three steps: key generation, encryption, and decryption. SSHv2 requires the asymmetric algorithm RSA-2048 with 2,048 bits (617 decimal digits), the largest of the RSA integers. The RSA algorithm is used in the validation of Juniper Networks signed binaries and is also available and used with the **ssh** command.

Copyright © 2016, Juniper Networks, Inc.

SHA-1—A Secure Hash Algorithm (SHA) standard defined in FIPS PUB 180-1 (SHA-1). Developed by NIST, SHA-1 produces a 160-bit hash for message authentication.

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

Related Documentation

- Understanding FIPS Self-Tests on page 11
- Understanding Zeroization to Clear System Data for FIPS Mode on page 10
- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 20

Understanding Zeroization to Clear System Data for FIPS Mode

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

The Crypto Officer initiates the zeroization process by entering the **request system zeroize** operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer. (To zeroize the system *before* enabling FIPS mode, use the **request system zeroize media** command.)

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

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

- Why Zeroize? on page 10
- When to Zeroize? on page 11

Why Zeroize?

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

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

Copyright © 2016, Juniper Networks, Inc.

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

- **Before FIPS operation.** To prepare your router for operation as a FIPS cryptographic module, perform zeroization after enabling FIPS mode and before FIPS operation.
- **Before non-FIPS operation.** To begin repurposing your router for non-FIPS operation, perform zeroization before disabling FIPS mode on the router or loading Junos OS packages that do not include FIPS mode.

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.

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

Related Documentation

- Zeroizing the System on page 35
- Disabling FIPS Mode on page 46
- *Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode*

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that a router 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 router performs the following series of known answer test (KAT) self-tests:

- **kernel_kats**—KAT for kernel cryptographic routines
- **md_kats**—KAT for libmd and libc
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **quicksec_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **ssh_ipsec_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

The KAT self-tests are performed automatically at startup and reboot, regardless of whether FIPS mode is enabled on the router. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and DSA 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.

Copyright © 2016, Juniper Networks, Inc.

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

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

Related Documentation

- Example: Configuring FIPS Self-Tests on page 47

Understanding FIPS Error States and System Panic

A router running Junos OS in FIPS mode has certain operational restrictions such as the ability to load only integrity-checked software files and use only FIPS-approved cryptographic algorithms. To ensure correct operation, the router performs a series of FIPS self-tests.

The router performs additional tests as needed—for example, to ensure that randomly generated numbers are truly random and to verify manually entered keys (passwords).

If it fails a test, the router enters a FIPS error state known as *system panic*.

When a low-level cryptographic function cannot complete for lack of memory or another resource, a memory allocation error occurs. This error does not result in system panic.

FIPS errors that occur early in the boot cycle can prevent the system from successfully starting up. For this reason, keep alternate boot media up to date.

For details, see:

- FIPS System Panic on page 12
- Memory Allocation Error on page 13
- Error Recovery from Alternate Boot Media on page 13

FIPS System Panic

If a router fails a FIPS self-test, the router enters a FIPS error state known as *system panic*. The panic condition halts all cryptographic processing and stops all data output from the router. To clear the FIPS error, the router reboots, runs the FIPS self-tests, and if it passes all the tests, returns to normal operation.

If the router fails a self-test during a reboot from panic mode, the system stops booting and attempts to reboot. If the reboot is unsuccessful, the router attempts again to reboot, this time from available boot media.

During a system panic, only status messages are displayed on the console. For example, a FIPS error is logged as shown in the following example:

```
panic: pid 5090 (fips-error), uid 0, FIPS error 5: cannot verify certificate
PackageCA
```

The reboot after panic displays the following error message on the console:

```
savecore: reboot after panic: pid 5090 (fips-error), uid 0, FIPS error 5: cannot
 verify certificate PackageCA
```


Copyright © 2016, Juniper Networks, Inc.

The following error states create a system panic:

NOTE: These errors have only an extremely small chance of occurring.

- The router failed a known answer test (KAT).
- The random number is not random.
- Signature generation failed.
- Signature verification failed.
- Certificate verification failed.
- Encryption or decryption failed.
- An environment error occurred.
- An error occurred in a pair-wise conditional test.

Memory Allocation Error

A FIPS memory allocation error occurs when a low-level cryptographic function cannot finish processing for lack of memory or of another resource. This error causes the affected process to be terminated, but does not result in system panic.

FIPS memory failures are logged as follows:

```
Apr 15 23:08:15 shmoo /kernel: pid 6374 (fips-error), uid 0, FIPS error 9: RSA
verify memory allocation failed
```

Terminating the process clears the error so that the process can be run again.

Error Recovery from Alternate Boot Media

A Juniper Networks router running Junos OS in FIPS mode performs KAT self-tests at startup. If the router fails a KAT, the boot process stops and the router attempts to reboot. If the reboot is unsuccessful, the router attempts again to reboot, this time from available boot media.

If the alternate media are not functional, the router might not be able to start up at all. In that case, the Crypto Officer must remove the tamper-evident seal from the USB port and insert the removable boot media so that the system can boot normally and install Junos OS.

However, if the seal is broken, the router is no longer a FIPS cryptographic module. As Crypto Officer, you must reinstall and reconfigure Junos OS and enable FIPS mode.

For this reason, be sure to keep the alternate media on the router in a functional state by running the **request system snapshot** command after a successful upgrade.

Related Documentation

- *Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode*
- request system snapshot

Copyright © 2016, Juniper Networks, Inc.

Understanding Roles and Services for Junos OS in FIPS Mode

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

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

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

Crypto Officers and FIPS users perform all FIPS-mode-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode. Crypto Officer and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode.

For details, see:

- Crypto Officer Role and Responsibilities on page 14
- FIPS User Role and Responsibilities on page 15
- What Is Expected of All FIPS Users on page 15

Crypto Officer Role and Responsibilities

The Crypto Officer is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a router. The Crypto Officer 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 Crypto Officer administer the system in a secure manner by keeping passwords secure and checking audit files.

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

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

Copyright © 2016, Juniper Networks, Inc.

Among the tasks related to Junos OS in FIPS mode, the Crypto Officer is expected to:

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

FIPS User Role and Responsibilities

All FIPS users, including the Crypto Officer, can view the configuration. Only the user assigned as the Crypto Officer can modify the configuration.

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

FIPS users configure networking features on the router and perform other tasks that are not specific to FIPS mode. FIPS users who are not Crypto Officers can perform reboots and view status output.

What Is Expected of All FIPS Users

All FIPS users, including the Crypto Officer, must observe security guidelines at all times.

All FIPS users must:

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

Related Documentation

- Zeroizing the System on page 35
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 6

Copyright © 2016, Juniper Networks, Inc.

Understanding the Operational Environment for Junos OS in FIPS Mode

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

Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the router that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the router that requires a cryptographic boundary for FIPS 140-2 compliance is a separate cryptographic module. There are two types of hardware with cryptographic boundaries in Junos OS in FIPS mode: one for each Routing Engine and one for each encryption services PIC (AS II or Multiservices FIPS PIC). Each component forms a separate cryptographic module. Communications involving CSPs between these secure environments must take place using encryption.

The Junos OS in FIPS mode hardware environment has limitations that apply to cryptographic boundaries. The PC Card slot might have to be secured with a tamper-evident seal. For FIPS Level 1 operation, the Routing Engine must be sealed into the chassis by using tamper-evident labels. On some models, tamper-evident labels must be applied to other components as well. See the FIPS Level 1 Label Installation Instructions for details. The label kit must be ordered separately and the labels applied according to the instructions included in the kit.

Hardware configurations with two Routing Engines use IPsec and a private routing instance for communications between them. Encryption is also used for communications between the Routing Engines and the encryption services PICs. If an encryption services PIC is used for IPsec connections to other systems, the encryption services PIC must be enabled first. For more information about encryption services PICs, refer to the hardware documentation for the model of PIC installed on your system.

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

Software Environment for Junos OS in FIPS Mode

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

FIPS mode on M Series, MX Series, PTX Series, and T Series routers is available in Junos OS Release 14.1R4 and later. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on a router. The

Copyright © 2016, Juniper Networks, Inc.

Junos OS Release 14.1R4 image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning router.

For FIPS 140-2 compliance, we recommend that you delete all user-created files and data from (that is, *zeroize*) the system immediately after enabling FIPS mode.

Operating the router at FIPS Level 1 requires the use of tamper-evident labels to seal the Routing Engines into the chassis. Removal of either Routing Engine requires entering the FIPS maintenance role. For strict compliance, the module should be zeroized on entry to and exit from the FIPS maintenance role.

Installing the Junos-FIPS image 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
- rsh
- 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 or SSL/TLS as a remote access service. Transport Layer Security (TLS) is equivalent to Secure Sockets Layer (SSL) version 3, and Junos OS in FIPS mode is further restricted to FIPS-approved algorithms.

NOTE: In Junos OS in FIPS mode, user authentication data can be entered in plain text. During initial configuration, the Routing Engine-to-Routing Engine IPsec key can also be entered in plain text on the console (under manual key entry rules). Otherwise, all CSPs must enter and leave the cryptographic module in encrypted form. In general, configuration should be done with SSH or TLS connections.

NOTE: RADIUS and TACACS+ authentication functionalities are disabled for Junos OS in FIPS mode.

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

Copyright © 2016, Juniper Networks, Inc.

must be changed to SHA1, SHA256, or 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 (20 for SHA-1).

NOTE: **Do not attach the router to a network until the Crypto Officer completes configuration from the local console connection.**

In dual Routing Engine configurations, the Routing Engines do not communicate until IPsec is properly configured on each Routing Engine. The Crypto Officer should use the console of each Routing Engine for this purpose.

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

Critical Security Parameters

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

Zeroization of the system erases all traces of CSPs in preparation for operating the router or Routing Engine as a cryptographic module.

Table 4 on page 18 lists CSPs on routers running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroize	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session key used with SSH-2. and as a Diffie-Hellman private key. Encryption: 3DES, AES-128, AES-192, AES-256. MACs: HMAC-SHA-1, HMAC SHA1-96, HMAC SHA-2-256, HMAC SHA2-512. Key exchange: DH Group exchange (2048 ≤ key ≤ 8192), ECDH Prime curve NID_secp521r1 (NIST Curve P-521).	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-1, SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-1, SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.

Copyright © 2016, Juniper Networks, Inc.

Table 4: Critical Security Parameters *(continued)*

CSP	Description	Zeroize	Use
RE-to-RE authentication key	HMAC key (manual IPsec SA): HMAC-SHA1-96 (20 bit), HMAC-SHA2-256 (32-bit).	Zeroize/explicitly delete command.	Used to authenticate the RE-to-RE IPSec connection.
RE-to-RE encryption key	TDES key (manual IPsec SA).	Zeroize/explicitly delete command.	Used in IPSec connection between REs.
HMAC DRBG seed	Seed for deterministic randon bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

In Junos OS in FIPS mode, all CSPs must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the Crypto Officer, you can enter user authentication data in plain text. During initial configuration, you can also enter the IPsec keys for communication between internal Routing Engines or for logical communications between the Routing Engine and system processes in plain text on the console port (under manual key entry rules).

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

Local passwords are encrypted with the HMAC-SHA-1 algorithm. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

Related Documentation

- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 20
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 6
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 22
- Understanding Zeroization to Clear System Data for FIPS Mode on page 10

Copyright © 2016, Juniper Networks, Inc.

- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode on page 24
- *Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode*

Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode

The internal IPsec SA provides a secure way to mutually authenticate and encrypt communications between Routing Engines.

The cryptographic boundary on a router is the Routing Engine. For this reason, routers with dual (redundant) Routing Engines require an internal, manual IPsec security association (SA) configured on each Routing Engine for the Routing Engines to communicate with each other. The Crypto Officer must use the console of each Routing Engine to configure the IPsec SA. Only four parameters are required: SA direction, security parameter index (SPI), a key value for authentication, and a key value for encryption. The SAs must be identical. All values, including the keys, must be statically specified in the configuration and must match on both ends of the connection. For communication to take place, each Routing Engine must have the same configured options.

For details, see:

- SA Direction on page 20
- SPI on page 21
- IPsec Keys on page 21
- IPsec Limitations on page 21

SA Direction

The internal, manual IPsec SA established by you, the Crypto Officer, on a Routing Engine can have the same SPI, authentication key, and encryption key for inbound and outbound communication, or one set of values for the inbound tunnel and another set for the outbound tunnel:

- Bidirectional—Apply the same SA values in both directions between Routing Engines.
- Inbound—Apply the SA values only to the inbound IPsec tunnel.
- Outbound—Apply the SA values only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure two unidirectional IPsec tunnels, one in each direction.

NOTE: **We recommend that you use bidirectional IPsec tunnels.**

Copyright © 2016, Juniper Networks, Inc.

SPI

The SPI is an arbitrary value between 256 and 16,639 that uniquely identifies the SA to use at the receiving Routing Engine. The sending Routing Engine uses the SPI to identify and select the SA it uses to secure every packet. The receiving Routing Engine uses the SPI to identify and select the encryption algorithm and key it uses to decrypt packets.

IPsec Keys

The internal, manual IPsec SA established by you, the Crypto Officer, on a Routing Engine requires an authentication key with a minimum digest length of 20 bytes, as well as an encryption key. For this type of SA, both keys must be preshared hexadecimal values, and each requires a specific cryptographic algorithm:

NOTE: **We recommend that you use the hexadecimal keys for maximum key strength on Junos OS in FIPS mode.**

- Authentication algorithm
  - HMAC-SHA1-96 (40 characters)
  - HMAC-SHA2-256 (64 characters)

NOTE: **We recommend that you use the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.**

- Encryption algorithm
  - 3DES-CBC (48 characters)

You use the configuration mode command **prompt** to enter the value for each key twice. If the two entries do not match, the key is not set.

IPsec Limitations

On a router with Junos OS in FIPS mode enabled, you cannot configure IPsec SAs to use the IPsec Authentication Header (AH) Protocol or the Data Encryption Standard (DES) encryption algorithm. Instead, you must use the Encapsulating Security Payload (ESP) protocol for both encryption and authentication and the 3DES-CBC algorithm for encryption.

Related Documentation

- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 6
- For more information about IPsec, see the *Junos OS System Basics Configuration Guide*.

Copyright © 2016, Juniper Networks, Inc.

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

Ensure that the router is in FIPS mode before you configure the Crypto Officer or any users. All passwords established for users by the Crypto Officer 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—for example, 20 characters for SHA-1 authentication. For a list of supported cryptographic algorithms (ciphers), see "Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms" on page 6.
- **Password encryption.** To change the default encryption method from MD5 to SHA1, SHA256, or 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

Copyright © 2016, Juniper Networks, Inc.

popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**r00t**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

Related Documentation

- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 6
- Understanding the Operational Environment for Junos OS in FIPS Mode on page 16

Understanding Remote Access for Junos OS in FIPS Mode

When the router is in Junos OS in FIPS mode, only SSH is available as a remote access service. To secure the information sent on administrative connections, use SSHv2 for CLI configuration. For SSH configuration information, see the *Junos OS System Basics Configuration Guide*.

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

The Ethernet management (**MGMT**) port on the router is disabled by default. To use the MGMT port, you must enable the **em0** interface and assign it an IP address if you have not already done so. For more information, see the *Junos OS System Basics Configuration Guide*.

In Junos OS in FIPS mode, all critical security parameters (CSPs) must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the Crypto Officer, you can enter user authentication data in plain text. During initial configuration, you can also enter the IPsec keys for communication between internal Routing Engines in plain text on the console port (under manual key entry rules).

Related Documentation

- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode on page 24
- *Junos OS System Basics Configuration Guide*.

Understanding Event Logging for Junos OS in FIPS Mode

A secure Juniper Networks Junos operating system (Junos OS) environment requires the auditing of configuration changes through the system log (syslog).

In addition, if configuration changes are audited, Junos OS can:

Copyright © 2016, Juniper Networks, Inc.

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

Event logging for Junos OS in FIPS mode must capture the following events:

- Changes to secret data in the configuration
- Committed changes
- Login and logout of users
- System startup and shutdown

BEST PRACTICE: **We recommend that FIPS logging also include:**

- **Capturing all changes to the configuration**
- **Storing logging information remotely**

Related Documentation

- Configuring Event Logging for Junos OS in FIPS Mode on page 43

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode

In FIPS mode, a router operates as a nonmodifiable operational environment in which only files shipped as part of Junos OS can be executed.

In contrast to non-FIPS mode, Junos OS in FIPS mode:

- Conforms to FIPS 140-2.
- Establishes a cryptographic boundary depending on the router chassis type. On fixed-configuration chassis, the boundary is the router case. On modular chassis, the boundary is the Routing Engine.
- Requires special installation procedures.
- Mandates the use of internal, manual IPsec tunnels with specific requirements.
- Limits services used for remote access.
- Allows only the use of approved ciphers.
- Requires user logout on disconnect at the console.
- Sets strict requirements for passwords.
- Requires special system logging considerations.

Copyright © 2016, Juniper Networks, Inc.

- Disables the following Junos OS protocols and services so that you cannot configure them. Attempts to configure these services, or to load configurations with these services configured, result in a configuration syntax error.
  - finger
  - FTP
  - rlogin
  - rsh
  - Telnet
  - Trivial File Transfer Protocol (TFTP)
  - Transport Layer Security (TLS) protocol
  - xnm-clear-text

  If you try to load a configuration that includes statements not supported by Junos OS in FIPS mode, you see a warning message. For example, suppose you attempt to configure Telnet for remote access:

  ```
  [edit]
  crypto-officer@host:fips# set system services telnet
  ```

  You receive the following warning and cannot add the **system services telnet** statement to the loaded configuration:

  ```
  [edit]
  'telnet'
  warning: not allowed in JUNOS-FIPS; ignored
  ```

Related Documentation

- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 20
- Understanding Remote Access for Junos OS in FIPS Mode on page 23
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 6
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 22
- Understanding Event Logging for Junos OS in FIPS Mode on page 23
- Understanding FIPS Error States and System Panic on page 12
- Configuring the Console Port for FIPS Mode on page 42

How to Enable and Configure Junos OS in FIPS Mode—Overview

You, as Crypto Officer, can enable and configure Junos OS in FIPS mode on your router.

Before you begin enabling and configuring FIPS mode on the router:

- Verify the secure delivery of your router. See “Identifying Secure Delivery” on page 5.

Copyright © 2016, Juniper Networks, Inc.

- Apply tamper-evident seals. See *Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode*.

To enable and configure Junos OS in FIPS mode, perform the following tasks. Follow the links for instructions.

1. Install the Junos OS Release 14.1R4 image, if you have not already done so. See "Downloading and Installing Junos OS Software Packages (FIPS Mode)" on page 29.
2. Disable non-CLI user interfaces.
3. Erase old passwords and roll back configurations. Otherwise, zeroize the system. See "Zeroizing the System" on page 35.
4. Establish root password access according to FIPS guidelines. See "Establishing Root Password Access (FIPS Mode)" on page 36.
5. Enable FIPS mode, and commit.

   NOTE: **On routers with multiple Routing Engines, ensure that you always use the commit synchronize command to commit configuration changes.**

6. Set IPsec security association (SA) algorithms and keys.
7. Configure local login authentication for Crypto Officer access and other FIPS users. See "Configuring Crypto Officer and FIPS User Identification and Access" on page 38.
8. Configure the console port to log out automatically when you unplug the cable and require the root password for single-user mode. See "Configuring the Console Port for FIPS Mode" on page 42.
9. Configure FIPS logging to record events. See "Configuring Event Logging for Junos OS in FIPS Mode" on page 43.

After you as the Crypto Officer complete Junos OS in FIPS mode configuration, you can connect the router to the network and proceed with normal configuration.

Related Documentation

- Understanding the Operational Environment for Junos OS in FIPS Mode on page 16

Copyright © 2016, Juniper Networks, Inc.

PART 2

Implementing Junos OS in FIPS Mode for M, MX, PTX, and T Series Routers

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 2

Enabling and Configuring Junos OS in FIPS Mode

Downloading and Installing Junos OS Software Packages (FIPS Mode)

M Series, MX Series, PTX Series, and T Series routers can provide the security defined by Federal Information Processing Standards (FIPS) 140-2 Level 1. To operate in Junos OS in FIPS mode, the router must have the following software packages installed:

- Junos OS for M, MX, PTX, and T Series routers, Release 14.1R4
- Junos FIPS mode, Release 14.1R4

To install the Junos software packages, perform the following tasks:

1. Download the Junos OS package and the Junos-FIPS software package from http://www.juniper.net/support/downloads/junos.html.
2. Connect locally to the active Routing Engine console port on the router.
3. Copy the Junos OS and Junos-FIPS software packages to the Routing Engine or Routing Engines.
4. Upgrade the router to Junos OS in FIPS mode by using the **request system software add reboot junos-juniper-14.1R4-fips.tgz** command. The router reboots with Junos OS in FIPS mode and becomes a cryptographic module. For more details about adding system software, see the *Junos Installation and Configuration Guide*.

Copyright © 2016, Juniper Networks, Inc.

5. Enable FIPS mode.

```
[edit]
user@host# set system fips level 1
```

6. Commit the configuration:

NOTE: If the router terminal displays error messages about the presence of critical security parameters (CSPs), delete those CSPs, and then commit the configuration.

For routers with a single Routing Engine:

```
{master:0}[edit security]
root@host# delete ipsec
{master:0}[edit security]
root@host# commit
configuration check succeeds
[edit]
 'system'
   reboot is required to transition to FIPS level 1
commit complete
```

For routers with multiple Routing Engines:

```
{master:0[edit security]
root@host# delete ipsec
{master:0}[edit security]
root@host# commit synchronize
configuration check succeeds
[edit]
 'system'
   reboot is required to transition to FIPS level 1
commit complete
```

NOTE: For hardware configurations with dual Routing Engines, configure a manual IPsec SA for Routing-Engine-to-Routing-Engine communication. You cannot use the **commit synchronize** command until you have established an IPSec SA on each Routing Engine.

Copyright © 2016, Juniper Networks, Inc.

NOTE: For PTX Series routers, during the initialization of the Routing Engine, you must delete the following configuration setting from the file located in the **/etc/config/ptx-series-defaults.conf** path to enable commit synchronization to occur successfully between the Routing Engines:

```
system {
        services {
          tftp {
            connection-limit 16;
          }
        }
      }
```

Related Documentation

- Understanding the Operational Environment for Junos OS in FIPS Mode on page 16

Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode

In a Junos OS in FIPS mode environment, routers with two Routing Engines must use IPsec for internal communication between the Routing Engines. You configure internal IPsec after you install the Junos OS in FIPS mode. You must be a Crypto Officer to configure internal IPsec.

NOTE: You cannot configure DES-based IPsec SAs in Junos OS in FIPS mode. The internal IPsec SAs use HMAC-SHA1-96 authentication and 3DES-CBC encryption.

Manual SAs require no negotiation. All values, including the keys, are static and specified in the configuration. Manual SAs statically define the SPI values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.

NOTE: When the switch is in FIPS mode, you cannot use the **commit synchronize** command until you have established an IPsec SA on each Routing Engine.

As Crypto Officer, you configure an internal IPsec SA for communication between Routing Engines by creating an SA on each Routing Engine with the following statements at the **[edit security]** hierarchy level:

To configure internal IPsec, include the **security-association** statement at the **[edit security]** hierarchy level. You can configure parameters, such as the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the

Copyright © 2016, Juniper Networks, Inc.

receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
          encryption {
            algorithm 3des-cbc;
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
        }
      }
    }
  }
}
```

Tasks for configuring internal IPsec for Junos-FIPS are the following. You can configure the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

1. Configuring the SA Direction on page 32
2. Configuring the IPsec SPI on page 33
3. Configuring the IPsec Key on page 34

Configuring the SA Direction

To configure the IPsec SA direction in which manual SAs of the IPsec tunnels must be applied, include the **direction** statement at the **[edit security ipsec internal security-association manual]** hierarchy level:

```
direction (bidirectional | inbound | outbound);
```

The value can be one of the following:

- **bidirectional**—Apply the same SA values in both directions between Routing Engines.
- **inbound**—Apply these SA properties only to the inbound IPsec tunnel.
- **outbound**—Apply these SA properties only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure SA parameters for IPsec tunnels in both the inbound and outbound directions. The following example uses an inbound and outbound IPsec tunnel:

Copyright © 2016, Juniper Networks, Inc.

NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction inbound {
          protocol esp;
          spi 512;
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
          encryption {
            algorithm 3des-cbc;
            key hexadecimal 309fc4be20f04e53e011b00744642d3fe66c2c7c;
          }
        }
        direction outbound {
          protocol esp;
          spi 513;
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
          encryption {
            algorithm 3des-cbc;
            key hexadecimal b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7;
          }
        }
      }
    }
  }
}
```

Configuring the IPsec SPI

A security parameter index (SPI) is a 32-bit index that identifies a security context between a pair of Routing Engines. To configure the IPsec SPI value, include the **spi** statement at the **[edit security ipsec internal security-association manual direction]** hierarchy level:

```
spi value;
```

The value must be from 256 through 16,639.

Copyright © 2016, Juniper Networks, Inc.

Configuring the IPsec Key

NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

The distribution and management of keys are critical to using VPNs successfully. You must configure the ASCII text key values for authentication and encryption. To configure the ASCII text key, include the **key** statement at the **[edit security ipsec internal security-association manual direction encryption]** hierarchy level:

key (ascii-text *ascii-text-string* | hexadecimal *hexadecimal-string*);

For this type of SA, both keys must be preshared hexadecimal values, and each requires a specific cryptographic algorithm:

- Authentication algorithm
  - HMAC-SHA1-96 (40 characters)
  - HMAC-SHA2-256 (64 characters)
- Encryption algorithm
  - 3DES-CBC (48 characters)

Use the configuration mode command **prompt** to enter the hexadecimal value for each key twice. For example:

```
[edit]
root@host:fips# prompt security ipsec internal security-association manual direction
   bidirectional encryption key hexadecimal
```

Enter the key in hexadecimal format per specification when prompted, for example (this is only an example):

```
03ff016465666768696a6b6c6d6e6f707172737475767778
```

NOTE: You must enter the key hexadecimal value twice and the strings entered must match, or the key will not be set. The hexadecimal key is never displayed in plain text. We recommend that you use the IPsec keys as hexadecimal keys for maximum key strength and not as ASCII keys for Junos OS in FIPS mode.

Related Documentation

- *Example: Configuring Internal IPsec*

Copyright © 2016, Juniper Networks, Inc.

Zeroizing the System

The **request system zeroize** command is a standard Junos OS operational mode command that you can use to revert a router to the factory-default configuration. The operation unlinks all user-created data files, including customized configuration and log files, from their directories. The router then reboots and reverts to the factory-default configuration. Your device is not considered a valid cryptographic module until all critical security parameters (CSPs) have been entered while the device is running the Junos OS in FIPS mode.

BEST PRACTICE: You must zeroize the system to remove all plain-text passwords, secret data, and private keys and CSPs, when no longer required.

The security administrator runs 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, secret data, and private keys and CSPs for SSH, local encryption, local authentication, IPsec, and SNMP.

To zeroize your device:

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.

1. From the CLI, enter:

```
admin@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)
```

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

```
Erase all data, including configuration and log files?  [yes, no] (no)
yes
re1:
--------------------------------------------------------------------------
warning: zeroizing re1
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```

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

3. When the system finishes rebooting and performing self-tests, proceed with secure configuration.

Copyright © 2016, Juniper Networks, Inc.

Establishing Root Password Access (FIPS Mode)

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

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 22. When you enable FIPS mode in Junos OS on the router, you cannot configure passwords unless they meet this standard.

Local passwords are encrypted with the secure hash algorithm HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-512. 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.

After you log in, configure the root (superuser) password to be used to access the router as follows:

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

   ```
   % cli
     — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
   root@host:fips> configure
     Entering configuration mode
     [edit]
     root@host:fips#
   ```

2. To set the password format, include the **format** statement at the **[edit system password]** hierarchy level.

   ```
   [edit]
   root@host:fips# set system password format (sha1 | sha256 | sha512)
   ```

3. Configure a temporary root password so that you can commit the configuration changes.
4. Commit the configuration changes.
5. Reset the root password to meet FIPS requirements.

Copyright © 2016, Juniper Networks, Inc.

6. Change the password format to a FIPS-compliant hash algorithm:

   NOTE: When establishing root password access after zeroization, the password format must be changed from the default of **md5**. MD5 is not a FIPS-compliant hash algorithm.

   a. Configure the FIPS-compliant hash algorithm for plain-text passwords by including the **format** statement at the **[edit system login]** hierarchy level and selecting **sha1**, **sha256**, or **sha512**:

      ```
      [edit]
      root@host:fips# set system login format (sha1 | sha256 | sha512)
      ```

   b. Configure a temporary root password to be able to commit the password format change. This password is hashed in the default format of MD5, and must be reset in Step 3.

   c. Commit the configuration:

      ```
      [edit]
      root@host:fips# commit
        commit complete
      ```

7. Configure the root password by including the **root-authentication** statement at the **[edit system]** hierarchy level and selecting one of the password options.

   - To configure a plain-text password, select the **plain-text-password** option. Enter and confirm the password at the prompts.

     ```
     [edit]
     root@host:fips# set system root-authentication plain-text-password
     New password: type password here
     Retype new password: retype password here
     ```

     Ensure that you follow the password guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 22.

   - To configure public keys for SSH authentication of root logins, use the **ssh-ecdsa** option. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as **root**, the public keys are referenced to determine whether the private key matches any of them.

   NOTE: The system is now ready to execute the **set system fips level 1** command.

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

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

Copyright © 2016, Juniper Networks, Inc.

Related Documentation

- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 22
- For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.

Configuring Crypto Officer and FIPS User Identification and Access

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

Configuring Crypto Officer 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 Crypto Officer. In most cases the **super-user** class suffices for the Crypto Officer.

To configure login access for a Crypto Officer:

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

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

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

   For a list of permissions, see Understanding Junos OS Access Privilege Levels.

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

   For example:

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

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 22, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

Copyright © 2016, Juniper Networks, Inc.

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

For example:

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

4. Optionally, display the configuration:

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

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

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

Otherwise, go on to "Configuring FIPS User Login Access" on page 39.

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 Crypto Officer you set up FIPS users. FIPS users can be granted permissions normally reserved for the Crypto Officer—for example, permission to zeroize the system.

To configure login access for a FIPS user:

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

```
crypto-officer@host:fips> configure
  Entering configuration mode
  [edit]
  crypto-officer@host:fips#
```

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

Copyright © 2016, Juniper Networks, Inc.

For a list of permissions, see Understanding Junos OS Access Privilege Levels.

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

For example:

```
[edit]
crypto-officer@host:fips# set system login user fips-user1 uid 6401 class operator
```

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 22, assign the FIPS user a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

For example:

```
[edit]
crypto-officer@host:fips# set system login user fips-user1 class operator authentication
  plain-text-password
```

4. Optionally, display the configuration:

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

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

```
[edit]
crypto-officer@host:fips# commit
crypto-officer@host:fips> exit
```

Otherwise, go on to "Configuring the Console Port for FIPS Mode" on page 42.

Related Documentation

- Understanding Roles and Services for Junos OS in FIPS Mode on page 14

Importing SSL Certificates for Junos XML Protocol Support

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

Copyright © 2016, Juniper Networks, Inc.

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router or switch: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the SSL protocol, you must copy an X.509 authentication certificate onto the router or switch, as described in this topic. You must also include the **xnm-ssl** statement at the **[edit system services]** hierarchy level.

NOTE: The xnm-ssl statement does not apply to standard IPsec services.

After obtaining an X.509 authentication certificate and private key, copy it to the router or switch by including the **local** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
local certificate-name {
   load-key-file (filename | url);
}
```

certificate-name is a name you choose to identify the certificate uniquely (for example, **Junos XML protocol-ssl-client-*hostname***, where ***hostname*** is the computer where the client application runs).

filename is the pathname of the file on the local disk that contains the paired certificate and private key (assuming you have already used another method to copy them to the router's or switch's local disk).

url is the URL to the file that contains a paired certificate and private key (for instance, on the computer where the Junos XML protocol client application runs).

NOTE: The CLI expects the private key in the ***URL-or-path*** file to be unencrypted. If the key is encrypted, the CLI prompts you for the passphrase associated with it, decrypts it, and stores the unencrypted version.

The load-key-file statement acts as a directive that copies the contents of the certificate file into the configuration. When you view the configuration, the CLI displays the string of characters that constitute the private key and certificate, marking them as SECRET-DATA. The load-key-file keyword is not recorded in the configuration.

Related Documentation

- *Configuring SSH Host Keys for Secure Copying of Data*
- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

Copyright © 2016, Juniper Networks, Inc.

Configuring the Console Port for FIPS Mode

You initially connect to your router through an RJ-45 serial cable plugged into the console port. From the console port, you can use the CLI to configure the router. By default, the console port is enabled.

For FIPS compliance, your user account must be automatically logged out when you unplug the serial console cable from a router running Junos OS in FIPS mode. Junos OS in FIPS mode automatically logs out of your user account when you disconnect because the **log-out-on-disconnect** configuration statement is enabled by default. Also, Junos OS in FIPS mode does not automatically disable root password recovery, so you must explicitly configure that by specifying the **insecure** configuration statement.

CAUTION: If you disable root password recovery by setting the insecure statement, the root password can be recovered only if the Crypto Officer logs in to the system and modifies the configuration by removing that setting.

To configure automatic logout on disconnection:

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

   ```
   crypto-officer@host:fips> configure
     Entering configuration mode
     [edit]
     crypto-officer@host:fips#
   ```

2. Configure the router to automatically log out of a user session when the console port cable is unplugged:

   ```
     [edit]
   crypto-officer@host:fips# set system ports console log-out-on-disconnect
   ```

3. Configure the router to disable root password recovery:

   ```
     [edit]
   crypto-officer@host:fips# set system ports console insecure
   ```

4. Optionally, display the configuration:

   ```
   [edit]
   crypto-officer@host:fips# edit system
   [edit system]
   ports {
     console {
       log-out-on-disconnect;
       insecure;
     }
   }
   ```

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

   ```
   [edit]
   crypto-officer@host:fips# commit
   ```


Copyright © 2016, Juniper Networks, Inc.

```
commit complete
crypto-officer@host:fips# exit
crypto-officer@host:fips> exit
```

Otherwise, go on to "Configuring Event Logging for Junos OS in FIPS Mode" on page 43.

Related Documentation

- For information about local console configuration and more information about console port options, see the *Junos OS System Basics Configuration Guide*.

Configuring Event Logging for Junos OS in FIPS Mode

The system log (syslog) files record system events in Junos OS.

BEST PRACTICE: **Because of the sensitive nature of information used to configure and operate a system running Junos OS in FIPS mode, we recommend that you as Crypto Officer log certain events and examine the logs frequently.**

For Junos OS in FIPS mode, we recommend that you as Crypto Officer configure the system log to record the following events. You can log more types of information, but these events are particularly important to the Junos OS in FIPS mode environment.

- All authorization events—stored in **/var/log/authlog** and **/var/log/auditlog**
- All interactive commands and configuration change events, including secrets—stored in **/var/log/auditlog**
- All events of moderate severity—stored in **/var/log/messages**

In Junos OS in FIPS mode, the actual secrets themselves are not logged. When Junos OS encounters secret information that it would ordinarily log, it replaces the secrets with the token **/* SECRET-DATA */**. For example, a secret string entered as part of the command line is not logged, but is replaced with the following token:

```
Feb 10 23:57:01 shmoo mgd[15558]: UI_CFG_AUDIT_SET_SECRET: User 'root' set: [system
 tacplus-server 172.17.12.120 secret]
Feb 10 23:57:01 shmoo mgd[15558]: UI_CMDLINE_READ_LINE: User 'root', command 'set
 system tacplus-server frodo secret /* SECRET-DATA */ '
```

The following system log configuration is recommended for Junos OS in FIPS mode:

```
[edit]
system {
   syslog {
      file authlog {
         authorization info;
      }
      file messages {
         any any;
      }
      file auditlog {
         authorization info;
```

```
        change-log any;
        interactive-commands any;
    }
  }
}
```

You can configure the system to log events to a local file or to a remote server:

- Configuring Event Logging to a Local File on page 44
- Configuring Event Logging to a Remote Server on page 45

Configuring Event Logging to a Local File

To configure the system to store the recommended information for Junos OS in FIPS mode, you create log files on the router called **authlog**, **auditlog**, and **messages**.

(You can also store event logs on a secure, remote server. For details, see "Configuring Event Logging to a Remote Server" on page 45.)

To configure the system to log the recommended events to local files on the router in the **/var/log/** directory:

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

   ```
   crypto-officer@host:fips> configure
     [edit]
     crypto-officer@host:fips#
   ```

2. Configure a file named **authlog** to store informational messages from the authorization system in **/var/log/authlog** on the router:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog file authlog authorization info
   ```

3. Configure a file named **auditlog** to store informational messages from the authorization system, all configuration changes, and all commands entered through the CLI—including secrets—in **/var/log/auditlog** on the router:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog file auditlog authorization info
   [edit]
   crypto-officer@host:fips# set system syslog file auditlog change-log any
   [edit]
   crypto-officer@host:fips# set system syslog file auditlog interactive-commands any
   ```

4. Configure a file named **messages** to store notices of all events of moderate severity in **/var/log/messages** on the router:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog file messages any any
   ```

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

   ```
   [edit]
   crypto-officer@host:fips# commit
     commit complete
   crypto-officer@host:fips# exit
   ```


Copyright © 2016, Juniper Networks, Inc.

```
crypto-officer@host:fips> exit
```

To view the contents of the log files, enter the following operational mode commands:

```
crypto-officer@host:fips> file show /var/log/authlog
crypto-officer@host:fips> file show /var/log/auditlog
crypto-officer@host:fips> file show /var/log/messages
```

Configuring Event Logging to a Remote Server

In addition to storing log files in the local **/var/log/** directory on the router (see "Configuring Event Logging to a Local File" on page 44), you can export the information in system log files to a secure, remote server.

BEST PRACTICE: We recommend that you store system log files remotely.

To configure the system to log the recommended events to a remote host:

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

   ```
   crypto-officer@host:fips> configure
     [edit]
     crypto-officer@host:fips#
   ```

2. Configure the system to import informational messages from the authorization system and store them on a remote host—for example, a host named **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog host Secure-Audit-Server authorization
    info
   ```

3. Configure the system to import all configuration changes and all commands entered through the CLI—including secrets—and store them on the remote host **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog host Secure-Audit-Server change-log
   any
   [edit]
   crypto-officer@host:fips# set system syslog host Secure-Audit-Server
   interactive-commands any
   ```

4. Configure the system to import all notices of events of moderate severity and store them on the remote host **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@host:fips# set system syslog host Secure-Audit-Server any notice
   ```

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

   ```
   [edit]
   crypto-officer@host:fips# commit
     commit complete
   crypto-officer@host:fips# exit
   crypto-officer@host:fips> exit
   ```

Copyright © 2016, Juniper Networks, Inc.

Related Documentation

- Understanding Event Logging for Junos OS in FIPS Mode on page 23
- For more information about system logging, see the *Junos OS System Basics Configuration Guide*.

Disabling FIPS Mode

As Crypto Officer, you might need to disable FIPS mode on your router to return it to non-FIPS operation.

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

To disable FIPS mode in Junos OS:

1. Log in to the router with your Crypto Officer password if you have not already done so:

   ```
   crypto-officer@host:fips>
   ```

2. Follow the instructions in"Zeroizing the System" on page 35 to zeroize the router.

3. When the system finishes rebooting, log back in to the router as the root user and enter configuration mode:

   ```
   — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
   root@host:fips> configure
   Entering configuration mode
   [edit]
   root@host:fips#
   ```

4. Commit the configuration change:

   ```
   [edit]
   root@host:fips# commit
   configuration check succeeds commit complete
   ```

Related Documentation

- How to Enable and Configure Junos OS in FIPS Mode—Overview on page 25

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 3

Administering Junos OS in FIPS Mode on a Juniper Networks Router

Example: Configuring FIPS Self-Tests

This example shows how to configure FIPS self-tests to run periodically.

Hardware and Software Requirements

- You must have administrative privileges to configure FIPS self-tests.
- The device must be running the evaluated version of Junos OS in FIPS mode software.

Overview

The FIPS self-test consists of the following suites of known answer tests (KATs):

- **kernel_kats**—KAT for kernel cryptographic routines
- **md_kats**—KAT for libmd and libc
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **ssh_ipsec_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

In this example, the FIPS self-test is executed at 9:00 AM in New York City, USA, every Wednesday.

NOTE: **Instead of weekly tests, you can configure monthly tests by including the month and day-of-month statements.**

Copyright © 2016, Juniper Networks, Inc.

When a KAT self-test fails, a log message is written to the system log messages file with details of the test failure. Then the system panics and reboots.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system fips self-test periodic start-time 09:00
set system fips self-test periodic day-of-week 3
```

Step-by-Step Procedure

To configure the FIPS self-test:

1. Configure the FIPS self-test to execute at 9:00 AM every Wednesday.

   ```
   [edit system fips self-test]
   user@host# set periodic start-time 09:00
   user@host# set periodic day-of-week 3
   ```

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

   ```
   [edit system fips self-test]
   user@host# commit
   ```

Results

From configuration mode, confirm your configuration by issuing the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show system
fips {
   self-test {
      periodic {
         start-time "09:00";
         day-of-week 3;
      }
   }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the FIPS Self-Test

Purpose Verify that the FIPS self-test is enabled.

Action Run the FIPS self-test manually by issuing the **request system fips self-test** command.

After issuing the **request system fips self-test** command, the system log file is updated to display the KATs that are executed. To view the system log file, issue the **file show /var/log/messages** command.

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


Copyright © 2016, Juniper Networks, Inc.

```
Oct 25 22:28:50  host kernel_kats[5358]: DES3-CBC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: HMAC-SHA2-256 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: SHA-2 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: AES128-CMAC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: AES-CBC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: FIPS Known Answer Tests passed

Oct 25 22:28:50  host md_kats[5360]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:28:50  host md_kats[5360]: HMAC-SHA2-256 Known Answer Test: Passed

Oct 25 22:28:50  host md_kats[5360]: FIPS Known Answer Tests passed

Oct 25 22:28:50  host openssl_kats[5362]: FIPS RNG Known Answer Test: Passed

Oct 25 22:28:57  host openssl_kats[5362]: FIPS DSA Known Answer Test: Passed

Oct 25 22:28:57  host openssl_kats[5362]: FIPS ECDSA Known Answer Test: Passed

Oct 25 22:28:58  host openssl_kats[5362]: FIPS ECDH Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: FIPS RSA Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: DES3-CBC Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: SHA-2 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: AES-CBC Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: ECDSA-SIGN Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: KDF-IKE-V1 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: FIPS Known Answer Tests passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: DES3-CBC Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: HMAC-SHA2-256 Known Answer Test:
Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: SHA-2 Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: AES-CBC Known Answer Test: Passed

Oct 25 22:29:01  host ssh_ipsec_kats[5364]: SSH-RSA-ENC Known Answer Test: Passed

Oct 25 22:29:03  host ssh_ipsec_kats[5364]: SSH-RSA-SIGN Known Answer Test: Passed

Oct 25 22:29:03  host ssh_ipsec_kats[5364]: KDF-IKE-V1 Known Answer Test: Passed
```

Copyright © 2016, Juniper Networks, Inc.

```
Oct 25 22:29:03  host ssh_ipsec_kats[5364]: FIPS Known Answer Tests passed
```

Meaning The system log file displays the date and the time at which the KATs were executed and their status.

Copyright © 2016, Juniper Networks, Inc.

PART 3

Configuration Statements and Operational Mode Commands for Junos OS in FIPS Mode

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 4

Configuration Statements for Junos OS in FIPS Mode

Copyright © 2016, Juniper Networks, Inc.

algorithm (FIPS)

Syntax algorithm 3des-cbc;

Hierarchy Level [edit security ipsec internal security-association manual direction encryption]

Release Information Statement introduced before Junos OS Release 7.4.

Description Select the encryption algorithm for the internal Routing-Engine–to–Routing-Engine IPsec security association (SA) configuration.

Options **3des-cbc**—Use a triple-Data Encryption Standard (3DES) cyclical block check (CBC) as the encryption algorithm.

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 31
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

 Copyright © 2016, Juniper Networks, Inc.

authentication (FIPS)

Syntax

```
authentication {
  algorithm (hmac-sha1-96 | hmac-sha2-256);
  key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IP Security (IPsec) authentication parameters for manual security association (SA).

NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Options **algorithm**—Hash algorithm that authenticates packet data. It can be one of the following:

- **hmac-sha2-256**—Produces a 256-bit digest.
- **hmac-sha1-96**—Produces a 160-bit digest.

key—Type of authentication key. It can be one of the following:

- **ascii-text key**—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
- **hexadecimal key**—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring Manual IPsec Security Associations for an ES PIC*

Copyright © 2016, Juniper Networks, Inc.

direction (FIPS)

Syntax

```
direction (bidirectional | inbound | outbound) {
  protocol esp;
  spi spi-value;
  encryption {
    algorithm 3des-cbc;
    key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
  }
}
```

Hierarchy Level [edit security ipsec internal security-association manual],
[edit security trusted-channel ipsec security-association manual]

Release Information Statement introduced before Junos OS Release 7.4.

Description Establish a manual security association (SA) for internal Routing-Engine–to–Routing-Engine communication.

Options

bidirectional—Apply the same SA values in both directions between Routing Engines.

inbound—Apply these SA properties only to the inbound IPsec tunnel.

outbound—Apply these SA properties only to the outbound IPsec tunnel.

The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 31
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

Copyright © 2016, Juniper Networks, Inc.

encryption (FIPS)

Syntax

```
encryption {
  algorithm 3des-cbc;
  key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the encryption parameters for internal Routing-Engine–to–Routing-Engine communication. The remaining statements are explained separately.

NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 31
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

fips (FIPS)

Syntax

```
fips {
  level level;
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Junos OS Federal Information Processing Standard (FIPS) mode features on a router.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Setting a Switch to FIPS Mode*
- *Disabling FIPS Mode*

Copyright © 2016, Juniper Networks, Inc.

format

Syntax format (md5 | sha1 | sha256 | sha512);

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the authentication algorithm for plain-text passwords.

Default For Junos OS, the default encryption format is **md5**. For Junos-FIPS software, the default encryption format is **sha1**.

Options The hash algorithm that authenticates the password can be one of these algorithms:

- Agreed technical requirements;
- Layout of the proposed physical and logical network topology;
- Protocols and equipment to be used;
- CoS and QoS functionality;
- Description of the devices and connectivity for End-User's sites;
- Further Juniper Networks' findings and recommendations, if applicable; and
- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.
- **sha256**—Produces a 256-bit digest.
- **sha512**—Produces a 512-bit digest.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Special Requirements for Junos OS Plain-Text Passwords*

Copyright © 2016, Juniper Networks, Inc.

ipsec (FIPS)

Syntax

```
ipsec {
  security-association {
    manual {
      direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        encryption {
          algorithm 3des-cbc;
          key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
        }
      }
    }
  }
  policy ipsec-policy-name {
    proposals [ proposal-names ];
  }
  proposal ipsec-proposal-name {
    authentication-algorithm (hmac-sha1-96 | hmac-sha2-256);
    encryption-algorithm 3des-cbc;
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  security-association name {
    dynamic {
      ipsec-policy policy-name;
      replay-window-size (32 | 64);
    }
    manual {
      direction (inbound | outbound | bi-directional) {
        authentication {
          algorithm (hmac-sha1-96 | hmac-sha2-256);
          key (ascii-text key | hexadecimal key);
        }
        auxiliary-spi auxiliary-spi-value;
        encryption {
          algorithm 3des-cbc);
          key (ascii-text key | hexadecimal key);
        }
        protocol (ah | esp | bundle);
        spi spi-value;
      }
    }
    mode (tunnel | transport);
  }
  traceoptions {
    file <files number> < size size>;
    flag all;
    flag database;
    flag general;
    flag ike;
    flag parse;
    flag policy-manager;
```

Copyright © 2016, Juniper Networks, Inc.

```
        flag routing-socket;
        flag timer;
    }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IPsec on encryption interfaces.

NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring Security Associations for IPsec on an ES PIC*

Copyright © 2016, Juniper Networks, Inc.

key (FIPS)

Syntax key (ascii-text *ascii-text-string* | hexadecimal *hexadecimal-string*);

Hierarchy Level [edit security ipsec internal security-association manual direction encryption]

Release Information Statement introduced before Junos OS Release 7.4.

Description The key used for the internal Routing-Engine–to–Routing-Engine IPsec security association (SA) configuration.

NOTE: We recommend that you use the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Options Only hexadecimal key is recommended to be used on Junos OS in FIPS mode.

ascii-text-string—The encrypted ASCII key.

hexadecimal-string—The encrypted hexadecimal key.

Required Privilege Level Crypto Officer—To add and view this statement in the configuration.

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 31
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

Copyright © 2016, Juniper Networks, Inc.

local

Syntax

```
local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
}
```

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

Options

certificate-namecertificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file *URL filename*—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Importing SSL Certificates for Junos XML Protocol Support on page 40

Copyright © 2016, Juniper Networks, Inc.

manual (Junos-FIPS Software)

Syntax

```
manual {
  direction (inbound | outbound | bi-directional) {
    authentication {
      algorithm (hmac-sha1-96 | hmac-sha2-256);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
      algorithm 3des-cbc;
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
```

Hierarchy Level [edit security ipsec security-association]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual IPsec SA.

NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- *Configuring an Internal IPsec Security Association for Dual Routing Engines*

Copyright © 2016, Juniper Networks, Inc.

protocol (Junos OS)

Syntax protocol (ah | esp | bundle);

Hierarchy Level [edit security ipsec proposal *ipsec-proposal-name*],
[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bidirectional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IPsec protocol for a manual or dynamic SA.

NOTE: Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, Junos OS does not support authentication header (AH) and ESP header bundles.

In transport mode, Junos OS supports only Border Gateway Protocol (BGP).

Options **ah**—Authentication Header protocol

bundle—AH and ESP protocols

esp—ESP protocol (the **tunnel** statement must be included at the **[edit security ipsec security-association *sa-name* mode** hierarchy level)

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Example: Using IPsec to Protect BGP Traffic*
- *Configuring Manual IPsec Security Associations for an ES PIC*
- *Configuring an IPsec Proposal for an ES PIC*

Copyright © 2016, Juniper Networks, Inc.

security (FIPS)

Syntax

```
security {
  certificates {
    local certificate-name {
      certificate-key-string;
      load-key-file URL filename;
      }
    }
  ipsec {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          encryption {
            algorithm 3des-cbc;
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
          }
        }
      }
    }
    policy ipsec-policy-name {
      proposals [ proposal-names ];
    }
    proposal ipsec-proposal-name {
      authentication-algorithm (hmac-sha1-96 | hmac-sha2-256);
      encryption-algorithm 3des-cbc;
      lifetime-seconds seconds;
      protocol (ah | esp | bundle);
    }
    security-association name {
      dynamic {
        ipsec-policy policy-name;
        replay-window-size (32 | 64);
      }
      manual {
        direction (inbound | outbound | bi-directional) {
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text key | hexadecimal key);
          }
          auxiliary-spi auxiliary-spi-value;
          encryption {
            algorithm 3des-cbc;
            key (ascii-text key | hexadecimal key);
          }
          protocol (ah | esp | bundle);
          spi spi-value;
        }
      }
      mode (tunnel | transport);
    }
    traceoptions {
```

Copyright © 2016, Juniper Networks, Inc.

```
        file <files number> < size size>;
        flag all;
        flag database;
        flag general;
        flag ike;
        flag parse;
        flag policy-manager;
        flag routing-socket;
        flag timer;
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define security parameters for communication between internal Routing Engines.

Options The remaining statements are explained separately.

Required Privilege Level security—To view and add this statement in the configuration.

Related Documentation

- *Configuring Security Associations for IPsec on an ES PIC*

Copyright © 2016, Juniper Networks, Inc.

security-association (Junos-FIPS Software)

Syntax

```
security-association sa-name {
  dynamic {
    ipsec-policy policy-name;
    replay-window-size (32 | 64);
  }
  manual {
    direction (inbound | outbound | bi-directional) {
      authentication {
        algorithm (hmac-sha1-96 | hmac-sha2-256);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi-value;
      encryption {
        algorithm 3des-cbc;
        key (ascii-text key | hexadecimal key);
      }
      protocol ( ah | esp | bundle);
      spi spi-value;
    }
    mode (tunnel | transport);
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 31
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

Copyright © 2016, Juniper Networks, Inc.

spi (Junos OS)

Syntax spi *spi-value*;

Hierarchy Level [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the security parameter index (SPI) for a security association (SA).

Options ***spi-value***—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).

Range: 256 through 16,639

NOTE: Use the auxiliary SPI when you configure the protocol statement to use the bundle option.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Example: Using IPsec to Protect BGP Traffic*
- *Configuring Manual IPsec Security Associations for an ES PIC*

Copyright © 2016, Juniper Networks, Inc.

CHAPTER 5

Operational Commands for Junos OS in FIPS Mode

- request system zeroize

Copyright © 2016, Juniper Networks, Inc.

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 switches.
Option **media** added in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 12.2 for MX Series routers.
Command introduced in Junos OS Release 12.3 for the QFX Series.
Option **local** added in Junos OS Release 14.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

NOTE: The media option is not available on the QFX Series.

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.

NOTE: If you configure the **commit synchronize** statement at the **[edit system]** hierarchy level and issue a **commit** in the master Routing Engine, the master configuration is automatically synchronized with the backup. However, if the backup Routing Engine is down when you issue the **commit**, the Junos OS displays a warning and commits the candidate configuration in the master Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the master. A newly inserted backup Routing Engine automatically synchronizes its configuration with the master Routing Engine configuration.

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

Options

media—(Optional) In addition to removing all configuration and log files, causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and so on. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the **request system zeroize media**

Copyright © 2016, Juniper Networks, Inc.

operation can take considerably more time than the **request system zeroize** operation. However, the critical security parameters are all removed at the beginning of the process.

local—(Optional) Remove all the configuration information and restore all the key values on the active Routing Engine.

Required Privilege Level maintenance

Related Documentation

- *request system snapshot*
- *request system snapshot*
- *Reverting to the Default Factory Configuration for the EX Series Switch*
- *Reverting to the Rescue Configuration for the EX Series Switch*
- *Reverting to the Default Factory Configuration*
- *Reverting to the Rescue Configuration*
- *Reverting to the Default Factory Configuration by Using the request system zeroize Command*

List of Sample Output

request system zeroize on page 71
request system zeroize media on page 72

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

0 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 5d19h20m26s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Mar 11 2011 - 04:39:06)

Board: EX4200-24T 2.11
EPLD:  Version 6.0 (0x85)
DRAM:  Initializing (1024 MB)
FLASH: 8 MB

Firmware Version: --- 01.00.00 ---
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.4
(user@example.net, Fri Mar 11 03:03:36 UTC 2011)
```

Copyright © 2016, Juniper Networks, Inc.

```
Memory: 1024MB
bootsequencing is enabled
bootsuccess is set
new boot device = disk0s1:
Loading /boot/defaults/loader.conf
/kernel data=0x915c84+0xa1260 syms=[0x4+0x7cbd0+0x4+0xb1c19]


Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 11.1R1.8 #0: 2011-03-09 20:14:25 UTC

user@example.net:/volume/build/junos/11.1/release/11.1R1.8/obj-powerpc/bsd/kernels/
  JUNIPER-EX/kernel
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080
...
```

request system zeroize media

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

warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing fpc0

{master:0}
root> Waiting (max 60 seconds) for system process `vnlru' to stop...done
. . .
Syncing disks, vnodes remaining...2 4 2 4 3 2 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 14m50s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD:  Version 8.0 (0x82)
DRAM:  Initializing (512 MB)
FLASH: 8 MB
NAND:  No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
```


Copyright © 2016, Juniper Networks, Inc.

```
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.example.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
    user@example.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080<EMCP,TBEN,EN_MAS7_UPDATE>
real memory  = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
. . .
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s2a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20055 free (31 frags, 2503 blocks, 0.0% fragmentation)
zeroizing /dev/da0s1a ...
. . .
zeroizing /dev/da0s3d ...
. . .
zeroizing /dev/da0s3e ...
. . .
zeroizing /dev/da0s4d ...
. . .
zeroizing /dev/da0s4e ...
. . .

syncing disks... All buffers synced.
Uptime: 3m40s
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD:  Version 8.0 (0x82)
DRAM:  Initializing (512 MB)
FLASH: 8 MB
NAND:  No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
```

```
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.example.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
    user@example.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080 <EMCP,TBEN,EN_MAS7_UPDATE>
real memory  = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
. . .
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s1a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20064 free (48 frags, 2502 blocks, 0.1% fragmentation)
zeroizing /dev/da0s2a ...
. . .
Creating initial configuration...mgd: error: Cannot open configuration file:
/config/juniper.conf
mgd: warning: activating factory configuration
mgd: commit complete
mgd: ------------------------------------------------------------
mgd: Please login as 'root'. No password is required.
mgd: To start Initial Setup, type 'ezsetup' at the JUNOS prompt.
mgd: To start JUNOS CLI, type 'cli' at the JUNOS prompt.
mgd: ------------------------------------------------------------
Setting initial options:  debugger_on_panic=NO debugger_on_break=NO.
Starting optional daemons: .
Doing initial network setup:
. . .

Amnesiac (ttyu0)
```


Copyright © 2016, Juniper Networks, Inc.

PART 4

Index

Copyright © 2016, Juniper Networks, Inc.

Index

Symbols

A

B

C

D

E

F

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.

N

P

R

S

T

U

V

Z

Copyright © 2016, Juniper Networks, Inc.

Copyright © 2016, Juniper Networks, Inc.