JUNIPER NETWORKS

Junos® OS

Secure Configuration Guide for Common Criteria and Junos-FIPS

Release

10.0R3

Published: 2010-10-21
Part Number: October, Revision 2

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Secure Configuration Guide for Common Criteria and Junos-FIPS
Release 10.0

Writing: Betsy Lichtenberg, Katie Smith
Editing: Sonia Saruba, Nancy Kurahashi
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
15 October—Revision 2

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The 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

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html .

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

Table of Contents

List of Tables

About This Guide

This preface provides the following guidelines for using the *Junos® OS Secure Configuration Guide for Common Criteria and Junos-FIPS*:

Objectives

This guide provides an overview of Junos OS Common Criteria and Junos-FIPS protocols for securing the Junos Internet software and describes how to configure Junos OS Common Criteria and Junos-FIPS protocols on the router.

NOTE: For additional information about Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/.

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M Series, MX Series, and T Series routing platforms, or EX Series switches, routing platform.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)

- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Routing Platforms

For the features described in this manual, Junos OS currently supports the following routing platforms:

- M Series
- MX Series
- T Series
- EX Series

Using the Indexes

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines,* refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *Junos OS CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos System Basics Configuration 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*
Text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; 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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web 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 J-Web 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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 postsales 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/
- 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).

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

PART 1

Common Criteria

CHAPTER 1

Configuring Common Criteria Users

This part of the *Secure Configuration Guide* provides configuration and operational information to help you perform the tasks associated with effectively configuring a network of Juniper Networks routers in a Common Criteria environment. The Common Criteria environment is implemented as a series of rules for software configuration. There are three aspects to Common Criteria configuration:

- Configuring authorized users
- Logging events of interest
- Firewall filtering of managers

This chapter describes all of the steps necessary to configure users in a secure Junos OS Common Criteria environment. Policies and Firewall filters for Common Criteria operation are detailed in subsequent chapters of this guide. User types perform certain types of router configuration and operational tasks.

The Junos OS Release 10.0 software has been evaluated for Common Criteria operations. For details of the scope of the Junos OS 10.0R3 evaluation, see the *Security Target for Juniper Networks M-Series Multiservice Edge Routers, MX-Series Ethernet Services Routers, T-Series Core Routers and EX Series Ethernet Switches running Junos 10.0R3.10*.

NOTE: Because this part of the *Secure Configuration Guide* only covers Common Criteria configuration and operation, refer to other Junos OS hardware and software manuals for non-Secure-Junos OS configuration tasks. While Common Criteria configuration statements and commands are noted in other Junos OS hardware and software configuration guides, all details relating to Common Criteria operation are presented in this part of the *Secure Configuration Guide*.

The configuration guidelines and features described in this part apply to Junos OS. For more detailed information about Junos-FIPS configuration and operation, see “Introduction to Junos-FIPS” on page 27.

This section is not intended as a troubleshooting guide. However, you can use it with a broader troubleshooting strategy to identify Common Criteria network problems.

This chapter discusses the following topics:

Introduction to Common Criteria

Common Criteria is the internationally accepted replacement for the outmoded United States Department of Defense Orange Book security evaluations. Government agencies around the world as well as many other organizations require Common Criteria evaluation as part of their product selection process.

Common Criteria allows product vendors to describe the security functions they offer in a standard manner, and allows customers to describe the security functions they require. Common Criteria makes it possible to map these two sets of features to a meaningful suite of products.

The hardware must be located in a secure physical environment and users of all types should not reveal keys or passwords. Additionally, they should not allow written records or notes to be seen by unauthorized personnel.

For more information about Common Criteria, see **http://www.commoncriteriaportal.org**. This chapter contains information about the following topics:

Common Criteria Overview

Common Criteria (ISO/IEC 15408) is a “cookbook” that allows for considerable latitude in meeting specific functional requirements. A secure Junos OS environment targets several areas of concern to deliver Evaluation Assurance Level 3 (EAL3) security to users. These areas include:

- SHA-2 support—A secure Junos OS environment supports the SHA-2 family of cryptographic algorithms internally.
- Routing correctness—A secure Junos OS environment supports all routing protocols required by Common Criteria EAL3.
- Manager identification and authentication—Only system managers (superusers) can change the authentication data for locally authenticated users in a secure Junos OS environment.

- Configuration change accounting—Configuration changes in a secure Junos OS environment are audited through syslog or RADIUS/TACACS+.
- Management traffic separation—A secure Junos OS environment treats managers and the information they require differently from user traffic.

Acronyms and Terms

The following acronyms and terms apply to a secure Junos OS environment and are not necessarily Common Criteria-specific.

- EAL—Evaluation Assurance Level. An assurance requirement defined by Common Criteria. For example, EAL2 is Evaluation Assurance Level 2 and EAL3 is Evaluation Assurance Level 3. Higher levels have more stringent requirements.
- ECC—Elliptical Curve Cryptography. A public key algorithm technique applied over an elliptical curve (a mathematical expression). Operations over an elliptical curve are known to be faster, more secure, and provide equivalent security using a smaller number of bits.
- ECDH—Elliptical Curve Diffie-Hellman. Applies the Diffie-Hellman algorithm over an elliptical curve.
- ECDSA—Elliptical curve digital signature algorithm. Applies digital signatures over an elliptical curve.
- FIPS—Federal Information Processing Standard. FIPS-140-2 and FIPS 140-3 deal with security and cryptographic modules.
- KATS—Known Answer Test System. Used to validate the cryptographic algorithm implementation, typically for verifying FIPS compliance.
- TOE—Target of Evaluation. Used to identify the component under evaluation for compliance.

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

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 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 routing platform to verify the authenticity of the platform:

- Verify the routing platform was ordered using a purchase order. Routing platforms are never shipped without a purchase order.
- When a router is shipped, a shipment notification is sent to the email address provided by the customer when the order is taken. Verify that this email notification was received. Verify that the email 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 customer

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

Upgrading an M-, MX-, or T Series Router to Common Criteria

To upgrade a Juniper Networks M- and T Series router running Junos OS to Junos OS Common Criteria, perform the following tasks in the order listed:

1. Download the applicable Junos OS package and MD5 or SHA1 hash file from www.juniper.net/customers/support. The packages and hash values for Common Criteria certified software are listed in Table 3 on page 7.
2. Connect locally to the active Routing Engine console port.
3. Copy Junos OS to both Routing Engines if applicable.
4. Upgrade using the **request system software add reboot <*jinstall-package*>** command. For example, use the **request system software add reboot jinstall-10.0R3.10-domestic-signed.tgz** command. For more details about adding system software, see the *Junos Installation and Configuration Guide*.

NOTE: The router must be rebooted before the software upgrade takes effect. Make sure you include the reboot switch with the request system software add command. Alternatively, after the software has been loaded, you can issue the request system reboot to reboot the router.

- When upgrading from Junos OS Release 6.4, you should use the **no-validate** option on the supported Junos OS Release 10.0 software modules. You can validate upgrades to supported Junos OS Release 10.0 modules from Junos OS Release 7.*x*. Upgrade to supported Junos OS Release 8.3 modules from Junos OS Release 6.4 using the **request system software add reboot <*jinstall-package*>-domestic-signed.tgz** command. For example, use the **request system software add reboot jinstall-10.0R3.10–domestic-signed.tgz** command.

Table 3: Common Criteria Junos OS Release 10.0R3 for M Series, MX Series, and T Series Routers

Software Package Name	MD5 Hash Value	SHA1 Hash Value
jinstall-10.0R3.10-domestic-signed.tgz	696537f882d551da629b2152987d85fd	1de0ac21f37913d173136149dd2b27242de38a60

For more details about installing Junos OS, see the *Junos OS Installation and Upgrade Guide*.

Upgrading an EX Series Switch to Common Criteria

To upgrade a Juniper Networks EX Series switch running Junos OS to Junos OS Common Criteria, perform the following tasks in the order listed:

1. Download the applicable Junos OS package and MD5 or SHA1 hash file from www.juniper.net/customers/support. The packages and hash values for Common Criteria certified software are listed in Table 4 on page 7.
2. Connect locally to the active Routing Engine console port.
3. Copy Junos OS locally or to a server that is accessible by the router during the installation process.
4. Upgrade using the **request system software add validate unlink reboot** *source***/juniper-ex-10.0R3.10**command. If the software is installed from a local directory on the router, *source* has the format ***/pathname***. If the software is installed from a remote location, *source* has the format **ftp://*hostname/pathname*** or **http://*hostname/pathname***.

Table 4: Common Criteria Junos OS Release 10.0R3 for EX Series Switches

Software Package Name	MD5 Hash Value	SHA1 Hash Value
jinstall-ex-3200-10.0R3.10-domestic-signed.tgz	b1ce04c521ca6b2a5078a9f45c99f7b2	8408c091c68370e5fe90d645dcefae487d58f15c
jinstall-ex-4200-10.0R3.10-domestic-signed.tgz	1caff48beed9ae173890c9f250025701	083429e2f0d815ccf6a6ac9be6a1f0044413d5f9

Table 4: Common Criteria Junos OS Release 10.0R3 for EX Series Switches *(continued)*

Software Package Name	MD5 Hash Value	SHA1 Hash Value
jinstall-ex-8200-10.0R3.10-domestic-signed.tgz	0e0db7bf381181ca848748338ba772d2	0383708793b3118a558e9df63e587af822dc6de9

Supported User Interface for Configuring Junos OS

For Common Criteria, the only supported way to log in and configure the router or switch is through the command-line interface (CLI). To conform to the certification, do not install the J-Web package on the device.

To conform to the certification on an EX Series Ethernet Switch, you must disable the J-Web and Junos Scope interfaces.

To disable the J-Web interface:

NOTE: If the J-Web package is not installed on the device, it is not possible to apply any web-management changes.

```
user@host>edit
user@host#delete system services web-management
user@host#commit
```

To disable the Junos Scope interface:

```
user@host>edit
user@host#delete system services xnm-ssl
user@host#delete system services xnm-clear-text
user@host#commit
```

Disabling the Console Port

By default, the console port on the router is enabled. You can use the console port to connect to the Routing Engine through an RJ-45 cable and use the command-line interface (CLI) to configure the router.

To disable to console port, log out of the console session if you are logged in through the console port. Then log in through any other access method and disable the console port.

You disable the console port with the **disable** statement:

```
[edit]
system {
   ports {
      console {
         disable;
      }
   }
}
```

NOTE: The console port is not the same as a dedicated management port. For strict compliance with the evaluated configuration, you should not configure fxp0.

For information about local console configuration, see the *Junos System Basics Configuration Guide*.

Protecting Management Connections

To secure the information sent on administrative connections, you should use secure shell protocol version 2 (SSHv2) for CLI configuration.

For information about configuring SSH, see the *Junos System Basics Configuration Guide*.

Choosing and Using Passwords

In general, a password must be:

- Easy to remember so that users are not tempted to write it down.
- Contain at least 8 characters of mixed alphanumerics and punctuation. There should be at least one change of case, one or more digits, or one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Weak passwords are:

- 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 that appears in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Louis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, or television shows.
- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (**f00t**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so should not be used.

Strong reusable passwords can be:

- Based on letters from a favorite phrase or word, and then
- Concatenated with other, unrelated words, along with added digits and punctuation.

Passwords should be changed from time to time.

Identifying and Authorizing Managers

In Junos OS for Common Criteria, users who are allowed to make changes to the router are called managers. Managers have read and write privileges over key operational components, such as counters, or configuration parameters, such as routing protocols. Some managers are considered superusers and have the ability to change configuration statements and security parameters in addition to other management tasks. Other users are not managers and have only read access (view permission) to some restricted parameters.

User accounts provide one way for users to access the router. (Users can access the router without accounts if RADIUS or TACACS+ servers are configured, as described in "Authorizing Users with RADIUS/TACACS+" on page 13.) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

- Username—(Required) Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the username.
- User's full name—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and should be unique on the router. If you do not assign a UID to a username, the software assigns one when you commit the configuration, using the lowest available number. You should ensure that the UID is unique. However, you can assign the same UID to different users. If you do, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- User access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in Table 5 on page 10.

Table 5: Default System Login Classes

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
superuser	all
unauthorized	none

- Authentication method or methods and passwords that the user can use to access the router—(Optional when RADIUS or TACACS+ are configured) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that Junos

OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

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

For information about SSH authentication, see the *Junos System Basics Configuration Guide*.

An account for the user **root** is always present in the configuration. For more information about user accounts, see the *Junos System Basics Configuration Guide*.

This section contains information about how to configure Common Criteria managers:

- Configuring Common Criteria Login Classes on page 11
- Authorizing Users with RADIUS/TACACS+ on page 13

Configuring Common Criteria Login Classes

This section contains information on configuring identification and authorization for the three types of login classes defined in Common Criteria documents:

- Configuring Superusers on page 11
- Configuring Operators on page 12
- Configuring Read-Only Users on page 12
- Configuring Users to View and Change the Idle-Timeout Value on page 13

Configuring Superusers

You configure Common Criteria superusers with the **superuser** login class. For example:

```
[edit]
system {
    login {
        user CC-superuser {
            full-name “Common Criteria Super User”;
            uid 1001;
            class superuser;
            authentication {
                encrypted-password “$1$pfKfjbHo0rjnnKL”; # SECRET-DATA
            }
        }
    }
}
```

Superusers have all permissions, including the ability to change the router configuration.

NOTE: When setting a password using a pre-encrypted format, the system manager is responsible for meeting or exceeding the minimal password strength requirements outlined in “Protecting Management Connections” on page 9.

Configuring Operators

You configure Common Criteria operators with the **operator** login class. For example:

```
[edit]
system {
   login {
      user CC-operator {
         full-name “Common Criteria Operator”;
         uid 1002;
         class operator;
         authentication {
            encrypted-password “$1$BaffophAt6rRxxvypF”; # SECRET-DATA
         }
      }
   }
}
```

Operators have the following permissions:

- clear—Clear learned network information.
- network—Access the network.
- reset—Reset or restart interfaces and daemons.
- trace—View trace file settings and audit logs.
- view—View current values and statistics.

The **trace** permission includes the ability to view audit logs. The **maintenance** permission adds the ability to modify the audit log directory, including file deletion. To limit audit log activity to view-only, use the **trace** permission. For information about audit logs, see “Configuring Common Criteria Event Logging” on page 17.

Operators cannot edit the configuration.

NOTE: When setting a password using a pre-encrypted format, the system manager is responsible for meeting or exceeding the minimal password strength requirements outlined in “Protecting Management Connections” on page 9.

Configuring Read-Only Users

You configure Common Criteria read-only users with the **read-only** login class. For example:

```
[edit]
system {
```



```
    login {
      user CC-read-only-user {
        full-name “Common Criteria Read-only User”;
        uid 1003;
        class read-only;
        authentication {
          encrypted-password “$1$oWlSRkewLtHeysAy”; # SECRET-DATA
        }
      }
    }
  }
```

Read-only users have only view permission and can only view current values and statistics.

NOTE: When setting a password using a pre-encrypted format, the system manager is responsible for meeting or exceeding the minimal password strength requirements outlined in “Protecting Management Connections” on page 9.

Configuring Users to View and Change the Idle-Timeout Value

Some login classes are predefined and the **idle-timeout** value cannot be changed for the class as a whole. By default, the **idle-timeout** value is set to 0 (the user will never be disconnected when the connection is idle). If you need to change the **idle-timeout** value for operators or read-only users, you should configure special classes of users with the desired **idle-timeout** values in minutes. For example:

```
[edit]
system {
  login {
    class idle-viewer {
      idle-timeout 30;
      permissions view; # This user class has only view permissions.
    }
    class idle-operator {
      idle-timeout 60;
      permissions [ clear network reset trace view ]; #This class is an operator
    }
  }
}
```

These user classes can now be assigned to users.

For more information about configuring users, see the *Junos System Basics Configuration Guide*.

Authorizing Users with RADIUS/TACACS+

For Common Criteria, you can configure RADIUS authentication, TACACS+ authentication, or both, as a method for authenticating users who attempt to access the router. You can also create template accounts to authenticate multiple users, configure a local fallback method in the event the RADIUS server is unavailable, and configure an authentication

order. For information about these topics, see the *Junos System Basics Configuration Guide*.

This section provides examples about how to configure user authentication on the router. This chapter includes the following topics:

Configuring RADIUS Authentication

To use RADIUS authentication on the router, configure information about one or more RADIUS servers on the network by including the **radius-server** statement at the **[edit system]** hierarchy level. For example:

```
[edit system]
radius-server 192.168.43.6 {
   accounting-port 4096;
   port 1812;
   retry 3;
   secret "$9$sdgoHjgYfmmLO9A"; # SECRET-DATA
   timeout 3;
}
```

You can specify a port number on which to contact the RADIUS server. By default, port number **1812** is used (as specified in RFC 2865).

You must specify a password in the **secret** statement. Passwords can contain spaces. The secret used by the local router must match that used by the server.

Optionally, you can specify the amount of time that the local router waits to receive a response from a RADIUS server (in the **timeout** statement), and the number of times that the router attempts to contact a RADIUS authentication server (in the **retry** statement). By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds. By default, the router retries connecting to the server three times. You can configure this to be a value in the range from 1 through 10 times.

To configure multiple RADIUS servers, include multiple **radius-server** statements.

To configure a set of users that share a single account for authorization purposes, create a template user.

You can also configure RADIUS authentication at the [**edit access**] and **[edit access profile]** hierarchy levels. Junos OS uses the following search order to determine which set of servers are used for authentication:

```
[edit access profile profile-name radius-server],
[edit access radius-server server-address],
[edit system radius-server ]
```

For more information, see the *Junos System Basics Configuration Guide*.

Configuring TACACS+ Authentication

To use TACACS+ authentication on the router, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level. For example:

```
[edit system]
tacplus-server 192.168.66.4 {
    port 4099;
    secret "$1$7fjhKJdlvnre9rnfJLdNeski"; # SECRET-DATA
    single-connection;
    timeout 3 ;
}
```

The port number is the TACACS+ server port number.

You must specify a secret (password) that the local router passes to the TACACS+ client by including the **secret** statement. Secrets can contain spaces. The secret used by the local router must match that used by the server.

You can optionally specify the length of time that the local router waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

You can optionally have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the **single-connection** statement.

NOTE: Early versions of the TACACS+ server do not support the single-connection option. If you specify this option and the server does not support it, Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

For more information about TACACS+, see the *Junos System Basics Configuration Guide*.

Miscellaneous RADIUS/TACACS+ Information

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the CLI username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

If you configure the router to be both a RADIUS and TACACS+ client (by including the **radius-server** and **tacplus-server** statements), you can prioritize the order in which the software tries the different authentication methods when verifying that a user can access

the router. For each login attempt, Junos OS tries the authentication methods in order, starting with the first one, until the password matches.

To configure the authentication order, include the **authentication-order** statement at the **[edit system]** hierarchy level. For example:

```
[edit system]
authentication-order [ radius tacplus password ];
```

You can specify one or more of the following in the preferred order, from first tried to last tried:

- **radius**—Verify the user using RADIUS authentication services.
- **tacplus**—Verify the user using TACACS+ authentication services.
- **password**—Verify the user using the password configured for the user with the **authentication** statement at the **[edit system login user]** hierarchy level.

If you do not include the **authentication-order** statement, users are verified based on their configured passwords.

For more information on RADIUS and TACACS+, see the *Junos System Basics Configuration Guide*.

CHAPTER 2

Configuring Common Criteria Event Logging

A secure Junos OS environment requires the auditing of configuration changes through syslog. RADIUS/TACACS+can also be used.

In addition, Junos OS can:

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

The logging for Common Criteria must capture the following events:

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

In addition, we recommend that logging also:

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

This chapter provides the following information about Junos OS for Common Criteria event logging:

Configuring Event Logging to a Local File

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

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

Common Criteria event logging should cover the same events as Junos-FIPS. For recommendations about which events to log, see “Recommended Junos-FIPS System Log Configuration” on page 39.

For more information about configuring event logging, see the *Junos System Basics Configuration Guide*.

Configuring Event Logging to a Remote Server

You configure the export of audit information to a secure, remote server with the **syslog** statement. This example sends logs to a remote host named **Secure-Audit-Server**:

```
[edit system]
syslog {
   host Secure-Audit-Server;
}
```

Common Criteria event logging should cover the same events as Junos-FIPS. For recommendations about which events to log, see “Recommended Junos-FIPS System Log Configuration” on page 39.

For more information about configuring event logging, see the *Junos System Basics Configuration Guide*.

Configuring NTP

Proper auditing of log integrity requires the use of accurate timestamps. Audit information in the form of logs sent to separate servers can be compared to detect tampering. Junos OS for Common Criteria provides accurate timestamping with the use of the Network Time Protocol (NTP).

You configure NTP by including the **ntp** statement. For example:

```
[edit system]
ntp {
   authentication-key 1 type MD5
   value "$9$EgfcrvX7VY4ZEcwgoHjkP5Q3CuREyv87"; # SECRET-DATA
   boot-server 10.10.10.12 ;
   server 10.10.10.14 key 1 prefer;
   source-address 192.168.77.2;
}
```

If the source address is configured, it must be a valid IP address configured on one of the router interfaces.

For more information about configuring NTP, see the *Junos System Basics Configuration Guide*.

Logging Configuration Changes to Secrets

This section provides information on two aspects of logging configurationchanges:

Configuring Auditing of Configuration Changes

This example audits all changes to the configuration secret data and sends the logs to a file named **Audit-File:**

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

This example expands the scope of the minimum audit to audit all changes to the configuration, not just secret data, and sends the logs to a file named **Audit-File:**

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

For more information on system logging parameters and facilities, see the *Junos System Basics Configuration Guide*.

Example: System Logging of Configuration Changes

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

Example Common Criteria Configuration

```
[edit system]
location {
   country-code US;
```

```
    building B1;
}
...
login {
    message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
        user tester {
        uid 2000;
        class super-user;
        authentication {
            encrypted-password “$1$pRxmZhC0$5F.ysqVL4Z5G67yg4Af4L.”;
                # SECRET-DATA;
        }
    }
    password {
        format md5;
    }
}
radius-server 10.10.10.10 {
    secret “$9$jCkfz3nC0ORmfEyKvN-ikqPz39Ap” # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
...
...
```

Example Common Criteria Configuration Changes

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

```
user@host# show | compare
[edit system login user tester authentication]
-    encrypted-password “$1$pRxmZhC0$5F.ysqVL4Z5G67yg4Af4L.”; # SECRET-DATA
+    encrypted-password “$1$4iTht8rmdlfKJdMMmdU03nd0skKwdj”; # SECRET-DATA
[edit system login]
+    user tester2 {
+        uid 2001;
+        class operator;
+        authentication {
+            encrypted-password “$1$hJP42n6Q$6twaOvyLAjfkFvZ6ELKxpGW”;
                # SECRET-DATA
+        }
+    }
```

```
[edit system radius-server 10.10.10.10]
-    secret “$9$jCkfz3nC0ORmfEyKvN-ikqPz39Ap”; # SECRET-DATA
+    secret “$9$99ZiCORrlMXNbvWbb2oGq.Fn/C0BrHs”; # SECRET-DATA
```

Load Merge

This section assumes that the example Common Criteria configuration is loaded on a router running Junos OS. When a **load merge** command is executed to merge the contents of the example Common Criteria configuration changes with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 24 17:43:28  chow mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system radius-server 1.2.3.4
 secret]
Jul 24 17:43:28  chow mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system login user tester
authentication encrypted-password]
Jul 24 17:43:28  chow mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system login user tester2
authentication encrypted-password]
```

Load Replace

This section assumes that the example Common Criteria configuration is loaded on a router running Junos OS. When a **load replace** command is executed to merge the contents of the example Common Criteria configuration changes with the contents of the original configuration, the following audit logs are created concerning the secret data:

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

Load Override

This section assumes that the example Common Criteria configuration is loaded on a router running Junos OS. When a **load override** command is executed to merge the contents of the example Common Criteria configuration changes with the contents of the original configuration, the following audit logs are created concerning the secret data:

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

Load Update

This section assumes that the example Common Criteria configuration is loaded on a router running Junos OS. When a **load update** command is executed to merge the contents of the example Common Criteria configuration changes with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Jul 25 14:31:03  chow mgd[4153]: UI_LOAD_EVENT: User 'tester' is performing a 'load update'
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_OTHER: User 'tester' update: CC_config2.txt
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system radius-server 1.2.3.4
```

```
 secret]
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_OTHER: User 'tester' deactivate: [system radius-server
1.2.3.4 secret] ""
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system login user tester
authentication encrypted-password]
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_OTHER: User 'tester' deactivate: [system login user tester
 authentication encrypted-password] ""
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'tester' set: [system login user test
authentication encrypted-password]
Jul 25 14:31:03  chow mgd[4153]: UI_CFG_AUDIT_OTHER: User 'tester' deactivate: [system login user test
authentication encrypted-password] ""
```

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

Login and Logout Events Using SSH

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

```
Dec 20 23:17:35  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:42  bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53  bilbo sshd[16645]: Accepted password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53  bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at permission level
                                   'j-operator'
Dec 20 23:17:53  bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class 'j-operator' [16648]
Dec 20 23:17:56  bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit '
Dec 20 23:17:56  bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout
```

Logging of Audit Startup and Shutdown

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

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

CHAPTER 3

Configuring Common Criteria Firewall Filters

We recommend auditing of various types of security violations, including attempts to access the system from unauthorized locations. Junos OS allows configuration of firewall filters to detect such attempts and create audit log entries when they occur.

In Junos OS, management traffic is isolated from other types of traffic, such as user transit traffic, in several ways. Junos OS maintains a separate virtual address space for every authorized manager. Traffic separation is also accomplished when a separate management network is connected to the dedicated management port **fxp0**.

You should deploy firewall filters on management ports to limit access to authorized managers and locations. For more information about firewall filters, see the *Junos Policy Framework Configuration Guide*.

This chapter provides the following information about Junos OS firewall filters:

Filtering Authorized Managers by Source Address

This example firewall filter limits manager access to **ssh** access from a device with source address **192.168.14.33.** It is applied to the loopback (**lo0**) interface as an input filter, and logs and rejects (silently discards) any attempts to access the router that do not meet these conditions.

NOTE: This firewall filter is only an example; do not copy the addressing specifics and use them on an actual system.

Configure the policy options and firewall filter:

```
[edit firewall family inet]
filter CC_MGR_Access {
   term ssh–okay {
      from {
```

```
        source-address {
          192.168.14.33/32;
        }
        destination-port 22;
      }
      then accept;
    }
    term other–okay {
      from {
        destination-port[0–21 23–65535];
        then {
        accept;
      }
    }
  }
```

Apply as an input filter to **lo0**:

```
[edit interfaces lo0 unit 0 family inet]
filter {
  input CC_MGR_Access;
}
```

Filtering NTP Messages by Address

This example firewall filter limits Network Time Protocol (NTP) messages to those to and from a certain pair of addresses (NTP server and local router), in this case 11.50.2.4 and 11.50.2.5. The filter is applied to the dedicated management interface or the **fxp0** management interface as an input filter, and logs and rejects (silently discards) any messages that are not valid.

NOTE: This firewall filter is only an example; do not copy the addressing specifics and use them on an actual system.

Configure the firewall filter:

```
[edit firewall family inet]
filter CC_NTP_Access {
  term NTP_server {
    from {
      source-address {
        11.50.2.4/32;
      }
      destination-address {
        11.50.2.5/32;
      }
      destination-port 123;
    }
    then accept;
  }
  term other {
    from {
      destination-port [ 0-122 124-65535 ];
```

```
        }
        then accept;
      }
    }
```

Apply as an input filter to **lo0**:

```
[edit interfaces lo0 unit 0 family inet]
filter {
  input CC_NTP_Access;
}
```

Filtering BGP Peers

If BGP is configured, we recommend using a firewall filter to restrict BGP connections to configured BGP peers.

This example firewall filter limits all TCP connection attempts to port **179** , the BGP port, from all addresses except the configured BGP peers. The filter is applied to the loopback **lo0** interface as an input filter, and rejects (silently discards) any packets that are not valid.

NOTE: This firewall filter is only an example; do not copy the addressing specifics and use them on an actual system.

Configure the policy options and firewall filter:

```
[edit policy-options]
filter bgp_179 {
  term one {
    from {
      source-address {
        172.17.12.1/32;
      }
      destination-port 179;
    }
    then accept;
  }
}
```

Apply the input filter to **lo0**;

```
[edit interfaces lo0 unit 0 family inet]
filter {
  input bgp_179;
}
```

You can also configure MD5 authentication for BGP. For more information on BGP authentication, see *Junos Routing Protocols Configuration Guide*.

PART 2

Introduction to Junos-FIPS

CHAPTER 4

Junos-FIPS Environment

This part of the *Secure Junos Configuration Guide* provides configuration and operational information to help you perform the tasks associated with effectively configuring a network of Juniper Networks routers in a Federal Information Processing Standards (FIPS) 140-2 environment. The FIPS 140-2 environment is implemented as both hardware and software. Two major roles are defined:

- Junos-FIPS Users can add or remove Adaptive Services II (AS II) FIPS Physical Interface Cards (PICs).
- The Crypto Officer installs the Junos-FIPS software and sets up the keys and passwords for the system and Junos-FIPS Users.

Both user types can also perform normal router configuration tasks, such as configuring routing protocols and routing policies as individual user configuration allows.

NOTE: Because this guide only covers Junos-FIPS configuration and operation, and is not related to the release of any specific products running Junos OS, refer to other Junos OS hardware and software manuals for non-Junos-FIPS configuration tasks. While Junos-FIPS configuration statements and commands are noted in other Junos OS hardware and software configuration guides, all details relating to Junos-FIPS operation are presented in the *Junos-FIPS Configuration Guide*.

This guide is not intended as a troubleshooting guide. However, you can use it with a broader troubleshooting strategy to identify Junos-FIPS network problems.

This chapter discusses the following topics:

Overview of Junos-FIPS

Junos-FIPS is a version of Junos OS that complies with FIPS 140-2 documentation. The FIPS documents define, among other things, security levels for computer and networking equipment. U.S. Federal Government departments, and other organizations, use FIPS to evaluate the cryptographic capabilities of the equipment they consider for purchase. Cryptographic modules are validated against 11 separate areas of the FIPS 140-2 specification. An overall certification level is assigned based on the minimum level achieved in any area.

Although primarily aimed at environments requiring strict security, FIPS levels are increasingly enforced as qualifying criteria for all U.S. Federal Government contracts. Security-conscious private enterprises might also use FIPS levels as an equipment evaluation benchmark. FIPS levels also serve as a customer-neutral description of vendor requirements. Vendors can engineer security products to FIPS levels and extend the applicability and eligibility of these products across a broad customer base, thereby eliminating exhaustive and time-consuming customer-by-customer product qualification procedures.

FIPS levels are defined in the FIPS 140-2 standard. The Junos-FIPS software operates at FIPS Level 1 or FIPS Level 2. When FIPS Level 2 operation is planned, tamper-evident labels must be applied to detect Routing Engine removal. On some models, tamper-evident labels must be applied to other components as well. See the *FIPS Level 2 Label Installation Instructions* for details.

FIPS 140-2 compliance is established for defined cryptographic boundaries; for example, the Junos-FIPS software running on a Routing Engine. Another defined cryptographic boundary for FIPS compliance is the entire AS II FIPS PIC. FIPS 140-2 mandates that no critical security parameters (CSPs), such as passwords and keys, can cross these boundaries, for example, by display on a console or written to an external log file. Although all running configurations involve hardware, only the software running on the Routing Engine and the AS II FIPS PIC require FIPS 140-2 certification. Junos OS by itself meets FIPS Level 1 requirements, and meets FIPS Level 2 requirements with the addition of tamper-evident labels sealing the Routing Engine and, in some cases, other components, into the chassis. This allows a large selection of the Juniper Networks product range to be used in environments that require FIPS 140-2 support.

Junos-FIPS creates a nonmodifiable, limited operational environment compared to Junos OS. You cannot load non-Junos-FIPS modules on a system running Junos-FIPS.

NOTE: Certain Junos-FIPS releases are submitted to the National Institute of Standards and Technology (NIST) for certification. Certain other releases, such as maintenance releases, might not be certified by NIST. Check with the software download page for Junos-FIPS on the Juniper Networks Web site or the National Institute of Standards and Technology site at http://csrc.nist.gov/cryptval/140-1/1401val.htm to determine whether a release is NIST-certified.

Supported Roles and Services

Unlike Junos OS, which allows a wide range of capabilities for users, such as routing control or view-only, the FIPS 140-2 standard defines two important types of users. For the purposes of this guide, the FIPS 140-2 roles are defined in terms of Junos OS user capabilities. The Junos-FIPS user roles are:

- Crypto Officer—Installs the Junos-FIPS software and establishes keys and passwords for other users and software modules. The Crypto Officer also authorizes the AS II FIPS PICs. For more information about the Crypto Officer, see “Crypto Officer Guide” on page 45.
- User—Views and in some cases modifies the configuration and zeroizes AS II FIPS PICs. In this guide, these users are called *Junos-FIPS Users*. For more information about Junos-FIPS Users, see “Junos-FIPS User Configuration” on page 50.

All other user types defined for Junos-FIPS (for example, operator, administrative user, and so on) and services (for example, remote protocol peers for remote access) must fall into one of the two categories of Crypto Officer or Junos-FIPS User.

NOTE: The set of Junos-FIPS permissions that distinguish Crypto Officers from other Junos-FIPS Users are secret, security, maintenance, and control. For strict FIPS compliance, all users should be assigned to a login class that contains all or none of these permissions.

Junos OS documentation uses the term “maintenance” in an entirely different sense than FIPS 140-2. When in doubt, the broader Junos OS definition of the “maintenance” term should be assumed.

Junos-FIPS Hardware Environment

A Juniper Networks router running Junos-FIPS forms a special type of environment. Junos-FIPS establishes several *cryptographic boundaries* in the router and no CSPs can cross these boundaries using plain text. There are two types of hardware with cryptographic boundaries in Junos-FIPS: one for each Routing Engine and one for each AS II FIPS PIC. Each component forms a separate cryptographic module. Communications involving CSPs between these secure environments must take place using encryption.

The Junos-FIPS hardware environment has limitations that apply to cryptographic boundaries. The PCMCIA slot might have to be secured with a tamper-evident seal. For FIPS Level 2 operation, the Routing Engine must be sealed into the chassis using tamper-evident labels. On some models, tamper-evident labels must be applied to other components as well. See the *FIPS Level 2 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 IP Security ( ) and a private routing instance for communications between them. Encryption is also used for communications

between the Routing Engines and the AS II FIPS PICs. If the AS II FIPS PIC is used for IPSec connections to other systems, the AS II FIPS PIC must be enabled first. For more information about the AS II FIPS PIC, see the *AS II FIPS PIC Hardware Guide*.

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

Junos-FIPS Software Environment

The Junos-FIPS software environment is established after the Crypto Officer has successfully installed the Junos-FIPS software module. Junos-FIPS software is only available from a specific location at the Juniper Networks Web site and can be installed as an upgrade to a functioning Juniper Networks router. Supported routing platforms are the M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers running Junos OS 10.0R1. RE-850, RE-1000, RE-2000A, and RE-2000S Routing Engines are certified for use in the FIPS environment.

You can upgrade to Junos-FIPS only from Junos OS Release 6.4 or higher. You should zeroize the system and all AS II FIPS PICs before downgrading to a non-Junos-FIPS software version.

Operating the router at FIPS Level 2 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 Junos-FIPS disables many of the usual Junos OS protocols and services. In particular, you cannot configure the following services in Junos-FIPS:

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

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error. For an example of these syntax errors, see “Configuration Restrictions” on page 33.

You can use only **ssl** or **tls** as a remote access service. Transport Layer Security (TLS) is equivalent to secure sockets layer (SSL) version 3, and Junos-FIPS is further restricted to FIPS-approved algorithms.

All passwords established for users after upgrading to Junos-FIPS must conform to Junos-FIPS 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 not included in the other four categories, such as % and &). Attempts to configure passwords that do not conform to these rules will 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). For Junos-FIPS user configuration examples, see "Crypto Officer and Junos-FIPS User Configurations" on page 49.

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 will 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-FIPS because some CSPs might be shown in plain text.

Configuration Restrictions

Junos-FIPS IPSec security associations (SAs) cannot be configured to use the IPSEC authentication header (AH) only, or to use data encryption standard (DES) encryption.

If you try to load a configuration that includes statements not supported in Junos-FIPS, you will see a warning message. For example, if you attempt to configure **telnet** for remote access:

```
[edit]
system {
   services {
      telnet;
   }
}
```

You see the following warning:

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

The statement will not be added to the loaded configuration. For more information on Junos-FIPS limitations, see "Junos-FIPS Software Environment" on page 32.

Summary of Junos OS and Junos-FIPS Differences

There are several major differences between Junos OS and Junos-FIPS. Junos-FIPS forms a non-modifiable limited operational environment compared to Junos OS.

In general, when compared to Junos OS, Junos-FIPS:

- Conforms to FIPS 140-2
- Establishes cryptographic boundaries around Routing Engines and AS II FIPS PICs
- Defines rules for installing or removing Routing Engines or AS II FIPS PICs
- Requires special installation procedures
- Mandates the use of IPSec tunnels in many areas
- Limits services used for remote access
- Allows only the use of approved ciphers
- Requires user logout on disconnect at console
- Sets strict requirements for passwords
- Requires special system logging considerations

CHAPTER 5

Upgrading and Configuring Junos-FIPS

This chapter describes the major characteristics of Junos-FIPS, including the upgrade procedure. In this chapter, the term "cryptographic module" applies to Junos-FIPS running on the Routing Engine.

This chapter discusses the following topics:

Critical Security Parameters

Critical security parameters (CSPs) are defined as security-related information (including cryptographic keys and authentication data, such as passwords), the disclosure or modification of which can compromise the security of a cryptographic module or the security of the information protected by the module.

In Junos-FIPS, user authentication data can be entered in plain text. During initial configuration, the Routing-Engine-to-Routing-Engine IP Security (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 secure shell (SSH) or Transport Layer Security (TLS) connections.

Services such as RADIUS and TACACS+ can still use clear text because FIPS 140 Level 2 or below allows for authentication data to be sent in clear text. For strict compliance, the RADIUS or TACACS+ server secret must be 10 characters or longer.

Local passwords are encrypted using HMAC-SHA1. Password recovery is not possible in Junos-FIPS. Junos-FIPS cannot boot into single-user mode without the correct root password.

If Junos-FIPS encounters a FIPS error, this condition halts all cryptographic processing, stops data flows, creates a system panic, and displays only status messages on the console.

For example, a FIPS error is logged as:

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

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

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

Memory failures are logged as well:

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

Upgrading a Junos OS Router to Junos-FIPS

To upgrade a Juniper Networks router running Junos OS to Junos-FIPS, perform the following tasks in the order listed:

- Install the router under normal operating procedures. For more information, see the *Junos Installation and Configuration Guide*.
- Download the correct Junos-FIPS software package from **www.juniper.net**.
- Connect locally to the active Routing Engine console port.
- Copy the Junos-FIPS software to both Routing Engines.
- Upgrade to Junos-FIPS using the **request system software add reboot junos-juniper-7.2*-fips.tgz** command. There is no "-signed" version of the Junos-FIPS software. All Junos-FIPS software is signed. The router reboots in Junos-FIPS and becomes a cryptographic module. For more details about adding system software, see the *Junos Installation and Configuration Guide*.
  - When upgrading from Junos OS Release 6.4, you should use the **no-validate** option on the Junos-FIPS software module. You can validate upgrades to Junos-FIPS from Junos OS Release 7.*x*. Upgrade to Junos-FIPS from Junos OS Release 6.4 using the **request system software add reboot no-validate junos-juniper-7.2*-fips.tgz** command.
- For hardware configurations with dual Routing Engines, configure a manual IPSec security association (SA) for Routing-Engine-to-Routing-Engine communication. You cannot use the **commit sync** command until you have established an IPSec SA on each Routing Engine.

NOTE: Downgrading a Junos-FIPS cryptographic module to non-Junos-FIPS Junos OS is not supported.

Attempts to install non-Junos-FIPS Junos OS on a router running Junos-FIPS will generate the following error message:

```
junos-fips-user@host> request system software add jinstall-7.2B1.2-domestic-signed.tgz
WARNING: Package jinstall-7.2B1.2-domestic-signed is not compatible with this system.
WARNING: Please install a supported package (junos-juniper-*.tgz).
```

Juniper Networks does not support downgrades to non-Junos-FIPS software packages, but this might be necessary in certain test environments. You can install non-Junos-FIPS Junos OS from PC Card media.

Entering Multiuser Mode

When Junos-FIPS is booted into single-user mode, a reboot is necessary to enter multiuser mode for normal operation with all services fully functional. You cannot exit the single-user shell and allow the system to come up in multiuser mode. A reboot loads the IPSec kernel module necessary for Routing-Engine-to-Routing-Engine communications in a multiple Routing Engine configuration.

```
Hit [Enter] to boot immediately, or space bar for command prompt. Booting [kernel]
 in 1 second...
Type '?' for a list of commands, 'help' for more detailed help. ok boot -s
Copyright (c) 1996-2001, Juniper Networks, Inc. All rights reserved. Copyright
(c) 1992-2001 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
7.2I20050420_0432_sjg #3: 2005-04-20 04:32:35 UTC
    sjg@swift.juniper.net:/c/sjg/work/7.2R1/obj-i386/sys/compile/JUNIPER
Timecounter "i8254"  frequency 1193182 Hz
...(many lines deleted)
FIPS self tests completed.
kern.securelevel: -1 -> 1
System watchdog timer disabled
Enter root password, or ^D to go multiuser
```

NOTE: Do *not* exit the shell for multiuser mode in Junos-FIPS. You must reboot.

```
Password:
Enter full pathname of shell or 'recovery' for root password recovery or RETURN
for /bin/sh:
NOTE: to go to multiuser operation, exit the single-user shell (with ^D)
NOTE:  If you exit from this shell, the system will attempt to come up normally.
  However the securelevel has already been raised so kernel modules cannot be
loaded and this may prevent the system being fully functional.
The best way to bring the system up from here is to 'reboot'.
```

To run a shell with a normal view of the system:

```
chroot /junos /bin/sh
```

```
# reboot
Apr 21 05:10:46 init: Multiuser: old requested_transition==0x0 sighupped=0

Waiting (max 60 seconds) for system process `bufdaemon' to stop...stopped
Waiting (max 60 seconds) for system process `syncer' to stop...stopped
```

```
syncing disks...
done
Uptime: 1m26s
ata0: Spinning down devices. Please wait...
Rebooting...
```

NOTE: You must reboot Junos-FIPS from single-user mode to enter multiuser mode with all services intact.

Configuring the Junos-FIPS Router

To configure a Juniper Networks router running Junos-FIPS, the Crypto Officer performs the following tasks in the order listed:

- Establish a root password conforming to the Junos-FIPS password guidelines discussed in “Passwords and Supported Cipher Sets” on page 48.
- For strict FIPS compliance, delete all rollback configurations.
- For strict FIPS compliance, reset any existing user passwords to ensure encryption with FIPS algorithms.
- For strict FIPS compliance, reset all keys.
- Apply a tamper-evident seal to the PCMCIA slot on applicable router models.
- For FIPS Level 2 operation, apply a tamper-evident label to seal each Routing Engine into the chassis. On some models, tamper-evident labels must be applied to other components as well. See the *FIPS Level 2 Label Installation Instructions* for details. Tamper-evident labels are ordered separately and applied according to the instructions included in the label kit.
- Establish Crypto Officer and other Junos-FIPS User logins. For more information about Crypto Officer and Junos-FIPS User logins, see “Crypto Officer and Junos-FIPS User Configurations” on page 49.

  NOTE: The set of Junos-FIPS permissions that distinguish Crypto Officers from other Junos-FIPS Users are **secret**, **security**, **maintenance**, and **control**. All users should be assigned to a login class that contains all or none of these permissions.

- Every AS II FIPS PIC used for external IPSec must be authorized. AS II FIPS PICs can be used for services such as firewalls or Network Address Translation (NAT) without authorization, but all external IPSec tunnels require authorization. For more information about authorizing AS II FIPS PICs, see “Authorizing the AS II FIPS PIC” on page 41.
- Connect the router to the network and proceed with normal router configuration.

Errors and Error Status Messages

Junos-FIPS errors stop all data output from the entire cryptographic module and cause a module panic, except very early in the boot cycle. Errors that occur early in the boot cycle can prevent the system from successfully booting. Keep alternate boot media up-to-date using the **request system snapshot** command. For more information about this command, see the *Junos System Basics and Services Command Reference*.

Junos-FIPS uses only FIPS-approved cryptographic algorithms, and only after a series of self-tests, including Known Answer Tests. A self-test failure results in a Junos-FIPS error state.

All but one of the following Junos-FIPS error conditions will create a system panic condition:

- Known Answer Test failed
- Random Number is not random
- Signature generation failed
- Signature verification failed
- Certificate verification failed
- Encryption/decryption failed
- Environment error
- Error in pair-wise conditional test
- Memory allocation error

The memory allocation error aborts the process making the call. All other errors result in a system panic condition and stop all data output. All errors except for memory allocation errors have only an extremely small chance of occurring.

For information about AS II FIPS PIC errors, see “AS II FIPS PIC Errors” on page 43.

For more information about Junos OS errors in general, see the *Junos System Basics Configuration Guide*.

Recommended Junos-FIPS System Log Configuration

The system log files are used to log system events in Junos OS and Junos-FIPS. Due to the sensitive nature of information used to configure and operate a system running Junos-FIPS, you should log certain events and examine the logs frequently.

The following is a recommended system log configuration for Junos-FIPS. More types of information can be logged, but these events are particularly important to the Junos-FIPS environment.

```
[edit]
system {
   syslog {
```

```
        file authlog {
            authorization info;
        }
        file messages {
            any notice;
        }
        file auditlog {
            authorization info;
            change-log any;
            interactive-commands any;
        }
    }
}
```

This system log configuration logs all authorization events to the **/var/log/authlog** and **/var/log/auditlog** files. The audit log file also receives all interactive commands and configuration change events. All events of moderate severity are logged to the **/var/log/messages** file.

Junos-FIPS secrets are not logged. When secret information that would ordinarily be logged in Junos OS is encountered, the secrets are replaced 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 */ '
```

For more information about system logging, see the *Junos System Basics Configuration Guide*.

CHAPTER 6

Configuring the AS II FIPS PIC

Junos-FIPS requires the use of an Adaptive Services II (AS II) FIPS Physical Interface Card (PIC) for external IP Security (IPSec) connections (internal IPSec is used between dual Routing Engines). The AS II FIPS PIC also obtains critical security parameters (CSPs) from the Routing Engine after the PIC has been enabled (authorized) on the system. You should zeroize the AS II FIPS PIC before removing it from the chassis.

This chapter discusses the following AS II FIPS PIC topics:

Installing and Removing the AS II FIPS PIC

Crypto Officers are responsible for the proper handling of any AS II FIPS PICs installed in the router. An AS II FIPS PIC is required for external IPSec sessions (internal Routing-Engine-to-Routing-Engine IPSec sessions do not require an AS II FIPS PIC).

The AS II FIPS PIC holds the Juniper Networks root certificate authority (CA) certificate and the factory default password for the PIC.

You must enable (authorize) all AS II FIPS PICs before use, and zeroize them before removal. If you move the AS II FIPS PIC to another system, you must authorize it for the new system.

This section discusses the following AS II FIPS PIC topics:

Authorizing the AS II FIPS PIC

Before you can use an installed AS II FIPS PIC for external IPSec, the Crypto Officer must authorize it. Authorization enables the AS II FIPS PIC, generates the cryptographic keys used for mutual authentication of the Routing Engine and AS II FIPS PIC, and generates the session key used for encryption and decryption of CSPs sent from the Routing Engine. It also creates a database of installed AS II FIPS PICs by serial number and status (authorized, not authorized).

The following automatically occurs when the AS II FIPS PIC is authorized:

- Mutual authentication using IPSec takes place between the active Routing Engine and the authorized PIC based on the default password on the PIC.
- The Routing Engine and AS II FIPS PIC generate private-public key pairs and exchange their public keys over the secure IPSec session.
- The Routing Engine sends the authorized PIC a *new* password used for zeroization.

The **request services fips authorize pic** command enables the Crypto Officer to authorize each individual AS II FIPS PIC:

```
crypto-officer@host> request services fips authorize pic fpc-slot 2
    pic-slot 0
Authorization started.
PIC authorized successfully.
```

You cannot authorize all installed AS II FIPS PICs at once. You cannot "re-authorize" an installed AS II FIPS PIC that has already been authorized:

```
crypto-officer@host> request services fips authorize pic fpc-slot 2
    pic-slot 2
Command failed as PIC sp-2/2/0 is already enabled. You need to zeroize it first to enable
    it.
```

Obtaining the AS II FIPS PIC Status

You can determine the status of all installed AS II FIPS PICs with the **show services fips pic status** command:

```
crypto-officer@host> show services fips pic status
FPC/PIC slot      Serial number    Status
2/0               CC8691           Not authorized
2/2               CC8689           Authorized
```

Authorized AS II FIPS PICs use a secure channel to the Routing Engine to install the IPSec security association (SA) keys on the PIC. If the AS II FIPS PIC is not authorized, the IPSec SA installation aborts.

Zeroizing the AS II FIPS PIC

A symmetric session key (in 3DES) is generated in the Routing Engine every time the Routing Engine or AS II FIPS PIC is rebooted. This session key is encrypted and signed with an RSA key pair and pushed to the PIC. IPSec SA keys are sent to the PIC encrypted with the session key. To maintain the cryptographic boundary, core dumps are disabled in the AS II FIPS PIC. You can return the PIC to the "factory-shipped" state by zeroizing it.

Before you remove an authorized AS II FIPS PIC from the system, you should zeroize the PIC with the **request services fips zeroize** command:

```
crypto-officer@host> request services fips zeroize pic fpc-slot 2 pic-slot 0
Zeroization command sent to the PIC. Please check logs for the result.
```

Note that once the command is issued and the cryptographic boundary around the AS II FIPS PIC is broken, the result can no longer be reported directly to the user. You should allow about 40 seconds to zeroize an AS II FIPS PIC.

You cannot zeroize all installed AS II FIPS PICs at once. They must be zeroized one at a time. You also cannot zeroize an installed AS II FIPS PIC that has not been authorized:

```
crypto-officer@host> request services fips zeroize pic fpc-slot 2 pic-slot 2
Command failed as PIC sp-2/2/0 is not authorized yet.
```

AS II FIPS PIC Errors

Junos-FIPS errors stop all data output from the cryptographic module and cause the module to panic, except very early in the boot cycle. The AS II FIPS PICs react to the error either at image download or run time.

The AS II FIPS PIC image is downloaded from the Routing Engine and verifies the image signatures after a verification self-test is run on the PIC. If the self-test or image signature verification fails, the AS II FIPS PIC repeats the image download process. If the process fails again, or if the signature is missing from the image, the AS II PIC panics and reboots.

The AS II FIPS PIC software uses only FIPS-approved cryptographic algorithms, and only after a series of known answer self-tests. A self-test failure generates an AS II FIPS PIC error state.

The following AS II FIPS PIC errors create a panic:

- Know answer test failure
- Random number is not random
- Password authentication failure during AS II FIPS PIC authorization

Password authentication failure during authorization causes auto-zeroization of the AS II FIPS PIC, as well as a panic reboot.

The following AS II FIPS PIC errors during authorization create a system log report and clean up the error, but do not cause a panic reboot:

- SA installation failure due to lack of a session key to decrypt the IPSec SA keys received from the Routing Engine
- SA installation failure due to reception of unencrypted IPSec SA keys from the Routing Engine after the AS II FIPS PIC has been authorized
- Memory allocation error

For information about Junos-FIPS errors, see “Errors and Error Status Messages” on page 39.

CHAPTER 7

Crypto Officer Guide

There are two categories of users in Junos-FIPS:

- Junos-FIPS User—Configures the system and performs all non-Junos-FIPS-related operations.
- Crypto Officer—Zeroizes the system, authorizes AS II FIPS PICs for operation, and displays the status of installed AS II FIPS PICs. Only the Crypto Officer can load the Junos-FIPS software and establish initial user profiles and IP Security (IPSec) parameters.

This chapter describes how a Crypto Officer configures a Juniper Networks router running Junos-FIPS and administers the system in a secure manner.

This chapter discusses the following topics:

List of Algorithms

This section provides a descriptive list of cryptographic algorithms and terms for reference purposes. 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) is 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.
- AH—The authentication header (AH) is part of IPSec and provides an authenticity guarantee for packets. If an AH packet contains a correct checksum hash, and no other party knows the secret key the peers share, the packet was not spoofed by an imposter and the packet was not modified in transit. Junos-FIPS does not allow use of IPSec with AH only.
- 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.
- ESP—The Encapsulating Security Payload (ESP) is part of IPSec and provides a confidentiality guarantee for packets through encryption. 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.
- Hashing—A method of message authentication that applies a cryptographic technique over and over (iteratively) to a message of arbitrary length and produces a hash "message digest" or "signature" of fixed length that is appended to the message when sent.
- HMAC—Defined as "Keyed-Hashing for Message Authentication" in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. HMAC can use one of several iterated cryptographic hash functions such as MD5 or SHA-1 (designated as HMAC-MD5 and HMAC-SHA1), along with a secret key.
- IKE—The Internet Key Exchange (IKE) is part of IPSec and provides ways to securely negotiate the shared private keys that the AH and ESP portions of IPSec need to function properly. IKE employs Diffie-Hellman methods and is optional in IPSec (the shared keys can be entered manually at the endpoints).
- IPSec—The IP Security protocol (IPSec) is a standard way to add security to Internet communications. The secure aspects of IPSec are usually implemented in three parts: AH, ESP, and IKE.
- MAC—Any general method of message authentication code (MAC) that uses encryption to compute a digital fingerprint (signature) for the original message. The recipient recomputes the fingerprint and compares it to the sent fingerprint.
- SA—A security association (SA) in IPSec is a set of parameters used by IPSec to determine how the security protocols (AH and ESP) operate, such as the private keys. The SA can be established by IKE (and expire) or set by manual configuration (and does not expire). SAs are unidirectional and are created in pairs.
- SHA-1—A Secure Hash Algorithm (SHA) standard defined in FIPS PUB 180-1 (SHA-1). Developed by the National Institute of Science and Technology (NIST), SHA-1 (which effectively replaces SHA-0) produces a 160-bit hash for message authentication.

Longer-hash variants include SHA-224, SHA-256, SHA-384, and SHA-512 (all are sometimes grouped under the name “SHA-2”).

- SPI—A security parameter index (SPI) in IPSec is a numeric identifier used with the destination address and security protocol to identify an SA. When IKE is used to establish the SA, the SPI is randomly derived. When manual configuration is used for an SA, the SPI must be entered as a parameter.
- SSH—The Secure Shell (SSH) 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.
- SSL—The secure sockets layer (SSL) is an Internet standard method used to secure communications over the Internet. SSL was developed by Netscape for securing Web sessions, but there is nothing Web-specific about SSL. SSL has goals similar to SSH, but with several important differences in terms of cryptographic protection.
- TLS—Transport Layer Security (TLS) is an Internet standard method used to secure communications over the Internet. It is the name of a standard protocol based on SSL 3.0, and is defined in RFC 2246. TLS in Junos-FIPS uses FIPS-restricted cipher sets in a FIPS environment.
- 3DES (3des-cbc)—A data encryption standard from the 1970s, the original DES used a 56-bit key (cracked in 1997). It is now enhanced with three multiple stages, effective key lengths of about 112 bits, and is often implemented with cipher block chaining (cbc).

Crypto Officer Responsibilities

The Crypto Officer securely upgrades the router to Junos-FIPS and initializes the router before network connection. We also recommend that the Crypto Officer administer the system in a secure manner, for example, by keeping passwords secure, checking audit files, and so on.

Among other tasks, the Crypto Officer is expected to:

- Set the initial root password.
- Insert the compact flash card where appropriate.
- Apply a tamper-evident seal to the flash card slot.
- For FIPS Level 2 operation, apply a tamper-evident label to seal each Routing Engine into the chassis. On some models, tamper-evident labels must be applied to other components as well. See the *FIPS Level 2 Label Installation Instructions* for details. Tamper-evident labels are ordered separately and applied according to the instructions included in the label kit.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Enable any AS II FIPS PICs before use.
- Set up manual IPSec SAs for configuration with dual Routing Engines.

- Examine log and audit files for events of interest.
- Perform other Junos-FIPS-related tasks as needed.

User Assumptions and Responsibilities

This configuration guide assumes that users, including Crypto Officers, respect security guidelines at all times. Users are expected to:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.

This configuration guide makes the following assumptions about user behavior:

- Users are trusted.
- Users abide by all security guidelines.
- Users will not deliberately compromise security.
- Users behave responsibly at all times.

Passwords and Supported Cipher Sets

All passwords must conform to Junos-FIPS rules. You will see an error message if you attempt to configure passwords that do not conform to these rules.

For more information about Junos-FIPS passwords and supported cipher sets, see “Junos-FIPS Software Environment” on page 32.

Remote Access

You can use only **ssh** or **tls** as a remote access service. For more information on remote access restrictions, see “Junos-FIPS Software Environment” on page 32.

Removing Old Passwords

For strict FIPS 140-2 compliance, you should remove old passwords and rollback configurations after upgrading the router to Junos-FIPS. For more information about removing initial passwords and rollback configurations, see the *Junos System Basics Configuration Guide*.

Zeroizing the System

You run the **request system zeroize** command to zeroize the router. This command erases all configuration information on the Routing Engines and resets all key values. The entire

request system zeroize command process can be time-consuming (for example, it requires about 20 minutes for a 20-gigabyte Routing Engine hard drive), but all critical security parameters (CSPs) are removed within a few seconds. The physical environment must remain secure until the zeroization process completes.

NOTE: System zeroization should be performed with care. After the zeroization process completes, there is no data left on the Routing Engine hard drive. The router is essentially left in the factory default state, without any configured users or configuration files.

Operating the router at FIPS Level 2 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.

Run the **request system zeroize** command before loading non-Junos-FIPS Junos OS packages. Juniper Networks does not support downgrades to non-Junos-FIPS software packages, but this might be necessary in certain test environments. You can install non-Junos-FIPS Junos OS from PCMCIA media.

Crypto Officer and Junos-FIPS User Configurations

Crypto Officers and Junos-FIPS Users perform all Junos-FIPS-related configuration tasks and issue all Junos-FIPS-related commands. Crypto Officer and Junos-FIPS User configurations must follow Junos-FIPS guidelines. This section discusses the following topics relating to user login configurations:

- Crypto-Officer User Configuration on page 49
- Junos-FIPS User Configuration on page 50
- Logging Out on Disconnect on page 50

Crypto-Officer User Configuration

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

For FIPS 140-2 conformance, any Junos-FIPS user with the **secret**, **security**, **maintenance**, and **control** permission bits set is a Crypto Officer. In most cases the **super-user** class should suffice for the Crypto Officer.

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

The following is an example Crypto Officer user configuration:

```
[edit system]
login {
   user crypto-officer {
      uid 6400;
      class super-user;
```

```
    authentication {
      encrypted-password “$sha1$2048$abcdef$87dfg4FGpim85qrs ?;
    }
    class super-user {
      permissions all;
    }
  }
}
```

Junos-FIPS User Configuration

The Crypto Officer sets up Junos-FIPS Users. Junos-FIPS Users can be granted permissions normally reserved for the Crypto Officer, for example, permission to zeroize the system and individual AS-II FIPS PICs. The following is an example Junos-FIPS User configuration:

```
[edit system]
login {
  user junos-fips-user {
    uid 6401;
    class junos-fips;
    authentication {
      encrypted-password “$sha1$20532$dead$beefcafebabe ?;
    }
  }
  class junos-fips {
    permissions [ clear configure network reset view view-configuration ];
  }
}
```

Logging Out on Disconnect

When you disconnect the console from the router running Junos-FIPS, your user account must be automatically logged out for FIPS compliance. This is *not* the default behavior for Junos-FIPS. You must add the **log-out-on-disconnect** configuration statement:

```
[edit system]
ports {
  console {
    log-out-on-disconnect;
  }
}
```

You can configure other options for the console port connection. For more information about console port options, see the *Junos System Basics Configuration Guide*.

Configuring Internal IPSec

To configure IPSec SA for internal, Routing-Engine-to-Routing-Engine communication, include the following statements at the **[edit security]** hierarchy level:

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
```

```
            protocol esp;
            spi spi-value;
            authentication {
              algorithm hmac-sha1-96;
              key ascii-text ascii-test-string;
            }
            encryption {
              algorithm 3des-cbc;
              key ascii-text ascii-text-string;
            }
          }
        }
      }
    }
  }
```

This section describes the following tasks for configuring internal IPSec:

- Configuring the SA Direction on page 51
- Configuring the IPSec SPI on page 52
- Configuring the IPSec Key Values on page 52

Internal IPSec requires manual configuration by a Crypto Officer. For more information about configuring a user as Crypto Officer, see "Crypto Officer and Junos-FIPS User Configurations" on page 49.

A router with two Routing Engines must have an internal IPSec SA configured to enable communication between the Routing Engines. Only four parameters are required: SA direction, SPI value, and key values for authentication and encryption.

NOTE: You cannot configure DES-based SAs in Junos-FIPS.

Configuring the SA Direction

To configure the IPSec SA direction, include the **direction** statement at the **[edit security ipsec internal security-association manual]** hierarchy level:

```
[edit security ipsec internal security-association manual]
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 directions. The following example uses an inbound and outbound IPSec tunnel:

```
[edit security]
ipsec {
```

```
internal {
  security-association {
    manual {
      direction inbound {
        protocol esp;
        spi 512;
        authentication {
          algorithm hmac-sha1-96;
          key ascii-text "$9$I5/hyKX7v4aUM8aUjH5TRhS1vLdb2 ?;
        }
        encryption {
          algorithm 3des-cbc;
          key ascii-text "$.KL3rngIH7,theOPcn87lxfpe9GJKdme ?;
        }
      }
      direction outbound {
        protocol esp;
        spi 513;
        authentication {
          algorithm hmac-sha1-96;
          key ascii-text "$9$I5/hyKX7v4aUM8aUjH5TRhS1vLdb2 ?;
        }
        encryption {
          algorithm 3des-cbc;
          key ascii-text ".n87lngIH7,thxefpe9GJKdme.KL3rOPc ?;
        }
      }
    }
  }
}
```

NOTE: The use of unidirectional IPSec tunnels is not recommended.

Configuring the IPSec SPI

To configure the IPSec SPI value, include the **spi** statement at the **[edit security ipsec internal security-association manual direction]** hierarchy level:

```
[edit security ipsec internal security-association manual direction]
spi value;
```

The value must be in the range from **256** through **16639**.

Configuring the IPSec Key Values

The last parameters required for a router with two Routing Engines are the ASCII text key values for authentication and encryption. You must configure both. For each key, you must enter the key ASCII value twice and the strings entered must match or the key will not be set.

To configure the key, include the **key** statement at the **[edit security ipsec internal security-association manual direction authentication]** and **[edit security ipsec internal security-association manual direction encryption]** hierarchy level:

[edit security ipsec internal security-association manual direction encryption]
key ascii-text ***ascii-string***;

Example: Configuring IPSec

Configure a bidirectional IPSec SA with an SPI value of 512 and a key value conforming to the FIPS 140-2 rules:

```
[edit security]
ipsec {
   internal {
      security-association {
         manual {
            direction bidirectional {
               protocol esp;
               spi 512;
               authentication {
                  algorithm hmac-sha1-96;
                  key ascii-text “$9$I5/hyKX7v4aUM8aUjH5TRhS1vLdb2 ?;
               }
               encryption {
                  algorithm 3des-cbc;
                  key ascii-text “$9$90j.COIek8X7VevbYgoji1rh ?;
               }
            }
         }
      }
   }
}
```

The text following **ascii-text** is never displayed in plain text.

CHAPTER 8

Summary of Junos-FIPS Operational Mode Commands

This chapter describes the command-line interface (CLI) commands you can use to change and display the status of Junos-FIPS components.

request services fips authorize pic

Syntax request services fips authorize pic fpc-slot ***fpc-number*** pic-slot ***pic-number***

Release Information Command introduced before Junos OS Release 7.4.

Description Authorize an AS II FIPS PIC in a router running Junos-FIPS.

Options none—All information must be provided for command execution.

Required Privilege Level maintenance

Sample Output: Successful Case

```
crypto-officer@host> request services fips authorize pic fpc-slot 2 pic-slot 2
Authorization started.
PIC authorized successfully.
```

Sample Output: Failure Case

```
crypto-officer@host> request services fips authorize pic fpc-slot 2 pic-slot 2
Command failed as PIC sp-2/0/0 is already enabled. You need to zeroize it first
to enable it again.
```

request services fips zeroize pic

Syntax request services fips zeroize pic fpc-slot ***fpc-number*** pic-slot ***pic-number***

Release Information Command introduced before Junos OS Release 7.4.

Description Zeroize an AS II FIPS PIC in a router running Junos-FIPS.

Options none—All information must be provided for command execution.

Required Privilege Level maintenance

Sample Output: Successful Case

```
crypto-officer@host> request services fips zeroize pic fpc-slot 2 pic-slot 2
Zeroization command sent to the PIC. Please check logs for the result.
```

Sample Output: Failure Case

```
crypto-officer@host> request services fips zeroize pic fpc-slot 2 pic-slot 0
Command failed as PIC sp-2/0/0 is not authorized yet.
```

request system software add reboot junos-juniper-7.4*-fips.tgz

Syntax request system software add reboot junos-juniper-7.4*-fips.tgz

Release Information Command introduced before Junos OS Release 7.4.

Description Upgrade the Routing Engine to Junos-FIPS.

Options none—Upgrades the Routing Engine from Junos OS Release 7.*x* or higher and boots into Junos-FIPS.

no-validate—Do ***not*** validate the module when upgrading from Junos OS Release 6.4.

Required Privilege Level maintenance

Sample Output

```
crypto-officer@host> request system software add reboot
/var/tmp/junos-juniper-7.4releasedetails-fips.tgz
Installing package '/var/tmp/junos-juniper-7.4 releasedetails -fips.tgz'...
Verified jpfe-7.4 releasedetails. tgz signed by PackageProduction_7_2_0 Verified
 junos-boot-juniper-7.4 releasedetails .tgz signed by     PackageProduction_7_4_0
 Verified junos-juniper-7.4 releasedetails -fips-optest signed by
     PackageProduction_7_4_0 Available space: 69723 require: 36970 JUNOS 7.4
releasedetails  will become active at next reboot jpfe-7.4 releasedetails .tgz
will be installed after next reboot Saving package file in /var/sw/pkg/junos-7.4
 releasedetails .tgz ...Saving state for rollback ... Rebooting ...
```

request system zeroize

Syntax request system zeroize

Release Information Command introduced before Junos OS Release 7.4.

Description Zeroize Routing Engines.

Options none—Zeroizes all Routing Engines in Junos-FIPS. You must verify the request by typing **yes** to proceed. This command is restricted to Crypto Officers because the **maintenance** permission bit is one of the permission bits, along with **secret** and **control**, that distinguishes Crypto Officers from other Junos-FIPS Users.

Required Privilege Level maintenance

Sample Output

```
crypto-officer@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
re1:
--------------------------------------------------------------------------
warning: zeroizing re1
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```

show services fips pic status

Syntax show services fips pic status

Release Information Command introduced before Junos OS Release 7.4.

Description Display the status of all installed AS II FIPS PICs in a router running Junos-FIPS.

Options none—Entire command must be entered for execution.

Required Privilege Level maintenance

Sample Output

```
crypto-officer@host> show services fips pic status
FPC/PIC slot      Serial number    Status 2/0  CC8691          Not authorized
  2/2               CC8689           Authorized
   FPC/PIC slot      Serial number    Status 2/0 CC8691          Not authorized
```

CHAPTER 9

Summary of Junos-FIPS Configuration Statements

The following sections explain each internal Routing-Engine-to-Routing-Engine IPSec configuration statement for Junos-FIPS. The statements are organized alphabetically.

algorithm

Syntax algorithm 3des-cbc;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Select the authentication and encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPSec SA configuration.

Options ***hmac-sha1-96***—Use a 96-bit Hash Message Authentication Code (HMAC) based on Secure Hash Algorithm 1 (SHA1) as the encryption algorithm.

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

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

authentication

Syntax

```
authentication {
  algorithm hmac-sha1-96;
  key ascii-text ascii-text-string;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the authentication parameters for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

direction

Syntax

```
direction (bidirectional | inbound | outbound) {
    protocol esp;
    spi spi-value;
    authentication {
        algorithm hmac-sha1-96;
        key ascii-text ascii-test-string;
    }
    encryption {
        algorithm 3des-cbc;
        key ascii-text ascii-text-string;
    }
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Establish a manual 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.

Usage Guidelines See “Configuring the SA Direction” on page 51.

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

encryption

Syntax

```
encryption {
  algorithm 3des-cbc;
  key ascii-text ascii-text-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.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

internal

Syntax

```
internal {
  security-association {
    manual {
      direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        authentication {
          algorithm hmac-sha1-96;
          key ascii-text ascii-test-string;
        }
        encryption {
          algorithm 3des-cbc;
          key ascii-text ascii-text-string;
        }
      }
    }
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an internal SA for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

ipsec

Syntax

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

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual SA for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

key

Syntax key ascii-text *ascii-text-string*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the key used for the internal Routing-Engine-to-Routing-Engine IPSec SA authentication and encryption configuration.

Options **ascii-text** *ascii-text-string*—The encrypted ASCII text key.

Usage Guidelines See "Configuring the IPSec Key Values" on page 52.

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

manual

Syntax

```
manual {
  direction (bidirectional | inbound | outbound) {
    protocol esp;
    spi spi-value;
    authentication {
      algorithm hmac-sha1-96;
      key ascii-text ascii-test-string;
    }
    encryption {
      algorithm 3des-cbc;
      key ascii-text ascii-text-string;
    }
  }
}
```

Hierarchy Level [edit security ipsec internal security-association]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual SA for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring Internal IPSec" on page 50.

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

protocol

Syntax protocol esp;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the protocol used for the internal Routing-Engine-to-Routing-Engine IPSec SA configuration.

Options esp .

esp—Use the TCP/IP encapsulating security protocol (ESP).

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

security

Syntax

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

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define security parameters for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

security-association

Syntax

```
security-association {
  manual {
    direction (bidirectional | inbound | outbound) {
      protocol esp;
      spi spi-value;
      authentication {
        algorithm hmac-sha1-96;
        key ascii-text ascii-test-string;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text ascii-text-string;
      }
    }
  }
}
```

Hierarchy Level [edit **security ipsec internal**]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an SA for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Internal IPSec” on page 50.

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

spi

Syntax spi *spi-value*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the security parameter index (SPI) value used for the internal Routing-Engine-to-Routing-Engine IPSec SA configuration.

Options *spi-value*—Integer to use for this SPI.

Range: **256** through **16639**

Usage Guidelines See “Configuring the IPSec SPI” on page 52.

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

PART 3

Index

Index

Symbols

A

B

C

T

U

V

Z

Index of Statements and Commands