

Chapter 1

JUNOS-FIPS Environment

The *JUNOS-FIPS 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. There are two main sections to this guide: for JUNOS-FIPS Users and for the Crypto Officer.

- 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 the JUNOS software, refer to other JUNOS hardware and software manuals for non-JUNOS-FIPS configuration tasks. While JUNOS-FIPS configuration statements and commands are noted in other JUNOS 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 on page 4
- Roles and Services Supported on page 5
- The JUNOS-FIPS Hardware Environment on page 5
- The JUNOS-FIPS Software Environment on page 6
- Configuration Restrictions on page 7
- Summary of JUNOS and JUNOS-FIPS Differences on page 8

Overview of JUNOS-FIPS

JUNOS-FIPS is a version of the JUNOS software 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. The JUNOS software 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 non-modifiable, limited operational environment compared to the JUNOS software. 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.

Roles and Services Supported

Unlike the JUNOS software, 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 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 27.
- **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 32

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.

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

The 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.

The 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, M320, and T320 routers, and the T640 routing node.

You can upgrade to JUNOS-FIPS only from JUNOS 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 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 7.

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 31.



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 will get 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 “The JUNOS-FIPS Software Environment” on page 6.

Summary of JUNOS and JUNOS-FIPS Differences

There are several major differences between the JUNOS software and JUNOS-FIPS. JUNOS-FIPS forms a non-modifiable limited operational environment compared to JUNOS.

In general, when compared to the JUNOS software, 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