

## Chapter 4

# 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 on page 28
- Crypto Officer Responsibilities on page 29
- User Assumptions and Responsibilities on page 30
- Passwords and Supported Cipher Sets on page 30
- Remote Access on page 31
- Removing Old Passwords on page 31
- Zeroizing the System on page 31
- Crypto Officer and JUNOS-FIPS User Configurations on page 31
- Configuring Internal IPSec on page 33
- Example: Configuring IPSec on page 36
- Internal IPsec Configuration Statements on page 36
- Command Summary on page 43

## 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 software.
- 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 “The JUNOS-FIPS Software Environment” on page 6.

## Remote Access

---

You can use only `ssh` or `tls` as a remote access service. For more information on remote access restrictions, see “The JUNOS-FIPS Software Environment” on page 6.

## 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 software 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 software 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 32
- JUNOS-FIPS User Configuration on page 32
- Logging Out on Disconnect on page 33

## 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 `security` statement:

```
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;
            }
          }
        }
      }
    }
  }
}
```

You can include the statement at the `[edit]` hierarchy level.

This section describes the following tasks for configuring internal IPsec:

- Configuring the SA Direction on page 34
- Configuring the IPsec SPI on page 35
- Configuring the IPsec Key Values on page 35

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 31.

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:

```
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";
          }
        }
      }
    }
  }
}
```



## 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.COlek8X7VevbYgoji1rh";
          }
        }
      }
    }
  }
}
```

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

## Internal IPsec Configuration Statements

---

The following sections explain each internal Routing-Engine-to-Routing-Engine IPsec configuration statement. The statements are organized alphabetically.

### *algorithm*

<b>Syntax</b>	<code>algorithm 3des-cbc;</code>
<b>Hierarchy Level</b>	<code>[edit security ipsec internal security-association manual direction authentication]</code> , <code>[edit security ipsec internal security-association manual direction encryption]</code>
<b>Release Information</b>	Statement introduced before JUNOS Release 7.4.
<b>Description</b>	Select the authentication and encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec SA configuration.
<b>Options</b>	Only <code>hmac-sha1-96</code> is supported for authentication. Only <code>3des-cbc</code> is supported for encryption.
<b>Usage Guidelines</b>	See “Configuring Internal IPsec” on page 33.
<b>Required Privilege Level</b>	<code>maintenance</code> —To add and view this statement in the configuration.

**authentication**

<b>Syntax</b>	<pre>authentication {   algorithm hmac-sha1-96;   key ascii-text <i>ascii-text-string</i>; }</pre>
<b>Hierarchy Level</b>	[edit security ipsec internal security-association manual direction]
<b>Release Information</b>	Statement introduced before JUNOS Release 7.4.
<b>Description</b>	Define the authentication parameters for internal Routing-Engine-to-Routing-Engine communication.
<b>Options</b>	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring Internal IPSec” on page 33.
<b>Required Privilege Level</b>	maintenance—To view and add this statement in the configuration.

**direction**

<b>Syntax</b>	<pre>direction (bidirectional   inbound   outbound) {   protocol esp;   spi <i>spi-value</i>;   authentication {     algorithm hmac-sha1-96;     key ascii-text <i>ascii-test-string</i>;   }   encryption {     algorithm 3des-cbc;     key ascii-text <i>ascii-text-string</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security ipsec internal security-association manual]
<b>Release Information</b>	Statement introduced before JUNOS Release 7.4.
<b>Description</b>	Establish a manual SA for internal Routing-Engine-to-Routing-Engine communication.
<b>Options</b>	<p><b>bidirectional</b>—Apply the same SA values in both directions between Routing Engines.</p> <p><b>inbound</b>—Apply these SA properties only to the inbound IPSec tunnel.</p> <p><b>outbound</b>—Apply these SA properties only to the outbound IPSec tunnel.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “Configuring the SA Direction” on page 34.
<b>Required Privilege Level</b>	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 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 33.

**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 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 33.

**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 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 33.

**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 Release 7.4.

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

**Options** Only `ascii-text` is supported.  
*ascii-text-string*—The encrypted ASCII text key.

**Usage Guidelines** See “Configuring the IPsec Key Values” on page 35.

**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 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 33.

**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 Release 7.4.

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

**Options** Only esp is supported.

**Usage Guidelines** See “Configuring Internal IPSec” on page 33.

**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 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 33.

**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 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 33.

**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 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 35.

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

## Command Summary

---

### *request system zeroize*

**Syntax** request system zeroize

**Release Information** Statement introduced before JUNOS 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...
...
```

