

Chapter 3

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 on page 19
- AS II FIPS PIC Errors on page 21
- Command Summary on page 23

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 on page 20
- Obtaining the AS II FIPS PIC Status on page 20
- Zeroizing the AS II FIPS PIC on page 21

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 13.

Command Summary

request services fips authorize pic

Syntax	<code>request services fips authorize pic fpc-slot <i>fpc-number</i> pic-slot <i>pic-number</i></code>
Release Information	Statement introduced before JUNOS 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 0 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	<code>request services fips zeroize pic fpc-slot <i>fpc-number</i> pic-slot <i>pic-number</i></code>
Release Information	Statement introduced before JUNOS 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.

show services fips pic status

Syntax show services fips pic status

Release Information Statement introduced before JUNOS 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
```