Configuring FIPS

This chapter describes how to configure the Federal Information Processing Standards (FIPS) mode on Cisco NX-OS devices.

This chapter includes the following sections:

- About FIPS, on page 1
- Prerequisites for FIPS, on page 2
- Guidelines and Limitations for FIPS, on page 3
- Default Settings for FIPS, on page 3
- Configuring FIPS, on page 3
- Verifying the FIPS Configuration, on page 5
- Create 2048 bit RSA Key, on page 5
- Configuration Example for FIPS, on page 6
- Additional References for FIPS, on page 6

About FIPS

The FIPS 140–2 Publication, *Security Requirements for Cryptographic Modules*, details the U.S. government requirements for cryptographic modules. FIPS 140–2 specifies that a cryptographic module is a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain cryptographic algorithms as secure, and it identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functioning properly.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation)

implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

Pair-wise consistency test

This test is run when a public or private key-pair is generated.

Continuous random number generator test

This test is run when a random number is generated.

The Cisco TrustSec manager also runs a bypass test to ensure that encrypted text is never sent as plain text.

Note A bypass test failure on CTS-enabled ports causes only those corresponding ports to be shut down. The bypass test might fail because of packet drops caused by data path congestion. In such cases, we recommend that you try bringing up the port again.

FIPS Error State

When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these bootup tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

Prerequisites for FIPS

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the **sap hash-algorithm HMAC-SHA-1** command from the cts-manual or cts-dot1x mode.

Guidelines and Limitations for FIPS

FIPS has the following configuration guidelines and limitations:

- The user authentication mechanisms supported for SSH are usernames and passwords, public keys, and X.509 certificates.
- Your passwords should have a minimum of eight alphanumeric characters.
- Disable Radius and TACACS when FIPS mode is on. This is enforced due to OpenSSL in FIPS mode.

Default Settings for FIPS

This table lists the default settings for FIPS parameters.

Table 1: Default FIPS Parameters

Parameters	Default
FIPS mode	Disabled

Configuring FIPS

This section describes how to configure FIPS mode on Cisco NX-OS devices.

Enabling FIPs Mode

Beginning with Cisco NX-OS Release 7.0(3)I5(1), you can enable FIPS mode on the device.

Before you begin

Ensure that you are in the default VDC.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**fips mode enable** **Example:** `switch(config)# fips mode enable`	Enables FIPS mode. **Note** **fips mode enable** can be entered only when all LCs are online or else it leads to LC failure.

	Command or Action	Purpose

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	(Optional) **show fips status**
	Example:
	`switch# show fips status`
	`FIPS mode is enabled`
		Displays the status of FIPS mode.

Step 5	Required: **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 6	Required: **reload** **Example:** `switch# reload`	Reloads the Cisco NX-OS device. **Note** After you enable FIPS, a reboot is required for the system to operate in FIPS mode.

Disabling FIPS

You can disable FIPS mode on the device.

Before you begin

Ensure that you are in the default VDC.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no fips mode enable** **Example:** `switch(config)# no fips mode enable`	Disables FIPS mode.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose

Step 4	(Optional) **show fips status**
	Example:
	`switch# show fips status`
	`FIPS mode is disabled`
		Displays the status of FIPS mode.

Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 6	**reload** **Example:** `switch# reload`	Reloads the Cisco NX-OS device.

Verifying the FIPS Configuration

To display FIPS configuration information, perform one of the following tasks:

Command	Purpose
show fips status	Displays the status of the FIPS feature.

Create 2048 bit RSA Key

Steps to create a 2048 bit RSA key:

- `N9k-Switch# conf t`

  `Enter configuration commands, one per line. End with CNTL/Z.`
- `N9k-Switch(config)# no feature ssh`

  `XML interface to system may become unavailable since ssh is disabled`
- `N9k-Switch(config)# no ssh key rsa`
- `N9k-Switch(config)# ssh key rsa 2048`
- `New SSH Key has a bitcount of 2048:`

  `N9k-Switch(config)# show ssh key`

  `**********`

  `rsa Keys generated:Wed Apr 28 13:05:18 2021`

  `ssh-rsa  AAAAB3NzaC1yc2EAAAADAQABAAABAQDHpxEgZ9LwmbOEpJeJtLwqedmTLkZV7Setxb9D4xgO`

  `p2o2f6wt/48bPp/vLDGsxTF2PtLRtRSSDFNSQmkw9bg+MXvTpgNivdxWLjxtwo3YpYwPkBiReVmyrFgE`

  `UuBmV/sDfhJpHXLoH9lR2+y0L5w1OG3cJxMe30TI37O3M8fZPjrAtHgkUubfEpiTbcyEw+aIHf+chyoR`

```
eDJxcEdnlboiTDFR0/+jMUUM/vMtxd5x5DH3AO7htA/i8lvskrReR1CpX1sOOdcshmS57EEuEzR9cs+w

KSftQh6vLD802207T6+J7/+cXMVNQEbq0mCSzeTmOsuIQe8u9ZC24pgYzZ19

bitcount:2048

fingerprint:

SHA256:Am9861AIq5MzfSPQr4ZXGe0f5M9crnhk7HVZBXhMVBo

*************************************

could not retrieve dsa key information

*************************************

could not retrieve ecdsa key information

*************************************
```

Configuration Example for FIPS

The following example shows how to enable FIPS mode:

```
config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload
```

Additional References for FIPS

This section includes additional information related to implementing FIPS.

Standards

Standards	Title
FIPS 140-2	Security Requirements for Cryptographic Modules