# Configuring FIPS

The Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

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

This chapter includes the following sections:

## Configuration Guidelines

Follow these guidelines before enabling FIPS mode:

- Make your passwords a minimum of eight characters in length.
- Disable Telnet. Users should log in using SSH only.
- Disable remote authentication through RADIUS/TACACS+. Only users local to the switch can be authenticated.
- Disable SNMP v1 and v2. Any existing user accounts on the switch that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Disable VRRP.
- Do not configure FIPS and IPsec together on a switch. With FIPS enabled, if you configure IKE, then FCIP links will not come up.
- Delete all SSH Server RSA1 keypairs.
- Do not configure FIPS and RADIUS together on a switch.
- FIPS cannot function when RADIUS (MD5) is enabled. Hence you need to note the following:

Before you enable FIPS you need to disable RADIUS or select other authentication protocol other than MD5.

Before you enable RADIUS you need to disable FIPS if you need to use the RADIUS (MD5) authentication protocol.

# Enabling FIPS Mode

To enable FIPS mode, follow these steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal` | Enters configuration mode. |
| **Step 2** | **fips mode enable**<br>**Example:**<br>`switch(config)# fips mode enable` | Enables FIPS mode. |
| **Step 3** | **no fips mode enable**<br>**Example:**<br>`switch(config)# no fips mode enable` | (Optional) Disables FIPS mode. |

# Displaying FIPS Status

To view FIPS status, enter the **show fips status** command.

# FIPS Self Tests

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

**Note** FIPS power-up self-tests automatically run when FIPS mode is enabled by entering the fips mode enable command. A switch is in FIPS mode only after all self-tests are successfully completed. If any of the self-tests fail, then the switch is rebooted.

Power-up self-tests run immediately after FIPS mode is enabled. A cryptographic algorithm test using a known answer must be run for all cryptographic functions for each FIPS 140-2-approved cryptographic algorithm implemented on the Cisco Nexus 5500 and 5600 Family.

Using a known-answer test (KAT), a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

Conditional self-tests must be run 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-private keypair is generated

  .
- Continuous random number generator test—This test is run when a random number is generated.

Both of these tests automatically run when a switch is in FIPS mode.