CHAPTER 2

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.

Note Cisco MDS SAN-OS Release 3.1(1) and NX-OS Release 4.1(1b) or later implements FIPS features and is currently in the certification process with the U.S. government, but it is not FIPS compliant at this time.

This chapter includes the following topics:

Information About 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 MDS 9000 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 key-pair 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.

Guidelines and Limitations

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.
- Delete all IKE policies that either have MD5 for authentication or DES for encryption. Modify the policies so they use SHA for authentication and 3DES/AES for encryption.
- Delete all SSH Server RSA1 key-pairs.

Enabling FIPS Mode

Detailed Steps

To enable FIPS mode, follow these steps:

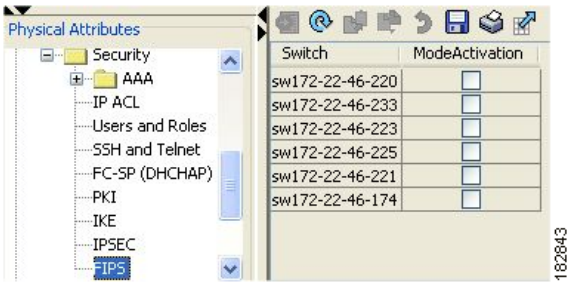
	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fips mode enable`	Enables FIPS mode.
	`switch(config)# no fips mode enable`	Disables FIPS mode.

To enable FIPS mode using DCNM-SAN, follow these steps:

Step 1 Expand **Switches** from the Physical Attributes pane. Expand **Security** and then select **FIPS**.

You see the FIPS activation details in the Information pane as shown in Figure 2-1.

Figure 2-1 FIPS Activation in DCNM-SAN



Step 2 Check the **ModeActivation** check box next to the switch for which you want to enable FIPS mode.

Step 3 Click **Apply Changes** to commit and distribute these changes.

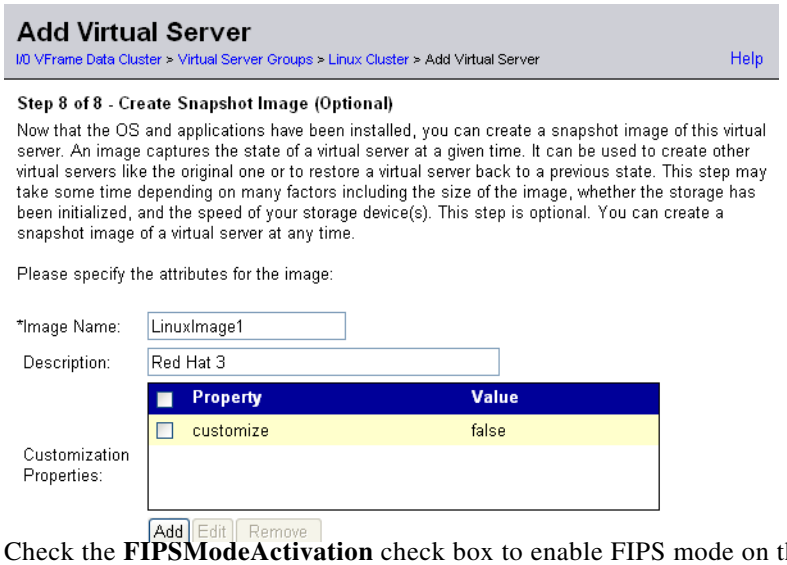
Step 4 Click **Undo Changes** to discard any unsaved changes.

To enable FIPS mode using Device Manager, follow these steps:

Step 1 Choose **Physical > System** or right-click and select **Configure.**

You see the System dialog box as shown in Figure 2-2.

Figure 2-2 System Dialog Box



Step 2 Check the **FIPSModeActivation** check box to enable FIPS mode on the selected switch.

Step 3 Click **Apply** to save the changes.

Step 4 Click **Close** to close the dialog box.

Verifying FIPS Configuration

Command	Purpose
show fips status	Displays the FIPS status.

For detailed information about the fields in the output from these commands, refer to the *Cisco DC-OS Command Reference*.

Field Descriptions for FIPS

FIPS

Field	Description
ModeActivation	To enable/disable FIPS mode on the device. FIPS 140-2 is a set of security requirements for cryptographic modules and it details the U.S. Government requirements for cryptographic modules. A module will comprise both hardware and software, eg a datacenter switching or routing module. The module is said to be in FIPS enabled mode when a request is recieved to enable the FIPS mode and a set of self-tests are successfully run in response to the request. If the self-tests fail, then an appropriate error is returned.